MX9 Reference Guide

E-EQ-MX9RG-C

2010 Copyright© by LXE®, Inc, An EMS Technologies Company. All Rights Reserved.

Notices

LXE Inc. reserves the right to make improvements or changes to published MX9 information at any time without notice. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, LXE assumes no liability resulting from any errors or omissions in this publication, or from the use of the information contained herein. Further, LXE Incorporated, reserves the right to revise this publication and to make changes to it from time to time without any obligation to notify any person or organization of such revision or changes.

Trademarks

Copyright © 2010 by LXE Inc., An EMS Technologies Company, 125 Technology Parkway, Norcross, GA 30092 U.S.A. (770) 447-4224

LXE® and **Spire**® are registered trademarks of LXE Inc.

RFTerm® is a registered trademark of EMS Technologies, Norcross, GA.

Microsoft®, ActiveSync®, MSN, Outlook®, Windows®, the Windows logo, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Intel and Intel XScale are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Summit Data Communications, Inc. Summit Data Communications, the Summit logo, and “The Pinnacle of Performance” are trademarks of Summit Data Communications, Inc.

The **Cisco** Square Bridge logo is a trademark of Cisco Systems, Inc.; Aironet, Cisco and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Java® and Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. or other countries, and are used under license.

The **Bluetooth**® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by LXE, Inc. is under license.

PowerScan is a registered trademark of Datalogic Scanning, Inc., located in Eugene, OR.

Symbol® is a registered trademark of Symbol Technologies. **MOTOROLA**® and the Stylized M Logo are registered trademarks of Motorola®, Inc.

Hand Held® is a registered trademark of Hand Held Products, Inc., located in Skaneateles Falls, NY.

When any part of this publication is in PDF format: “Acrobat ® Reader Copyright © 2010 **Adobe** Systems Incorporated. All rights reserved. Adobe, the Adobe logo, Acrobat, and the Acrobat logo are trademarks of Adobe Systems Incorporated” applies.

Other product names mentioned within this publication may be trademarks or registered trademarks of other companies.

Table of Contents

Introduction 1

Components 2

Front 2

Top 5

Bottom 5

Back 6

Trigger Handle 7

Handstrap 8

Label Locations 9

Hardware 10

System Hardware 10

Central Processing Unit 10

System Memory 10

Internal SD Memory Card 10

Video Subsystem 11

Power Supply 11

Input/Output Connector 11

Bluetooth 12

Audio Support 12

802.11 b/g and a/b/g Wireless Client 12

External Input/Output Port 12

COM Ports 13

Keypads 13

Modifier Keys 13

Expansion Slots 13

Power Key Functions 14

Status LEDs 15

System Status LED 15

Battery Charging Status LED 15

Alpha mode Status LED 15

Bluetooth Status LED 15

Scanner Status LED 16

Vibrate Indicator 17

Cold Storage 17

Heating Elements 17

Cables 17

Scanners and Imagers 18

Integrated Barcode Decoders ... 18
Tethered Barcode Decoders ... 18
Bluetooth Client Barcode Decoders ... 18
GPS Module ... 18
Power ... 19
Main Battery ... 19
External Power Supplies ... 19
AC/DC 15V Power Supply ... 20
Car Power Adapter ... 20
Replace CLA Fuse ... 20
Power Modes ... 21
On ... 21
User Idle ... 21
System Idle ... 22
Suspend ... 23
Suspend Primary Wake up Events ... 23
Wake Up Event Default Settings ... 24
Critical Suspend ... 24
Off ... 24
Software ... 25
Operating System ... 25
Windows CE 5.0 Operating System ... 25
General Windows CE Keyboard Shortcuts ... 25
Warmboot ... 26
Clearing Persistent Storage / Reset to Default Settings ... 26
Folders Copied at Startup ... 26
Saving Changes to the Registry ... 27
Software Load ... 28
Software Applications ... 28
Bluetooth (Optional) ... 28
LXE RFTerm (Optional) ... 28
MX9 Utilities ... 29
LAUNCH.EXE ... 29
LAUNCH.EXE and Persistent Storage ... 30
REGEDIT.EXE ... 30
REGLOAD.EXE ... 30
REGDUMP.EXE ... 30
WAVPLAY.EXE ... 30
PrtScrn.EXE ... 31

API Calls ... 31
Access Files on the Flash Card ... 31
Desktop Icons ... 32
Taskbar Icons ... 33
My Device Folders ... 33
Start Menu Program Options ... 34
Communication ... 35
ActiveSync Introduction ... 35
Connect and LXEConnect ... 35
Start FTP Server / Stop FTP Server ... 35
Summit ... 35
Certs ... 35
Command Prompt ... 36
Internet Explorer ... 36
Media Player ... 36
Microsoft Wordpad ... 36
Remote Desktop Connection ... 37
Transcriber ... 37
Windows Explorer ... 37
Taskbar ... 38
General Tab ... 38
Advanced Tab ... 39
Taskbar Icons ... 39
ActiveSync ... 41
Introduction ... 41
Initial Setup ... 41
Connect via USB ... 42
Cable for USB ActiveSync Connection: ... 42
Connect via Serial ... 43
Cable for Serial ActiveSync Connection ... 43
Connect via Wireless ... 43
Synchronizing from the Mobile Device ... 44
Explore ... 44
Backup Data Files using ActiveSync ... 44
Prerequisites ... 44
Serial Port Transfer ... 44
USB Transfer ... 44
Connect ... 44
Disconnect ... 45
Troubleshooting ActiveSync ... 46

Cold Boot and Loss of Host Re-connection ... 46
MX9 without Touchscreen ... 46
Configuring the MX9 with LXEConnect ... 47
Install LXEConnect ... 47
Using LXEConnect ... 49
Control Panel ... 50
About ... 52
Version Tab and the Registry ... 52
Language and Fonts ... 52
Identifying Software Versions ... 53
MAC Address ... 53
Accessibility ... 54
Administration - for AppLock ... 55
Introduction ... 55
Factory Default Settings - AppLock ... 56
Setup a New Device ... 57
Administration Mode ... 58
End User Mode ... 59
Passwords ... 59
End-User Switching Technique ... 60
Using a Stylus Tap ... 60
Using the Switch Key Sequence ... 60
Hotkey (Activation hotkey) ... 60
Application Configuration ... 61
Application Panel ... 62
Launch Button ... 64
Auto At Boot ... 64
Auto Re-Launch ... 65
Manual (Launch) ... 66
Allow Close ... 67
Match ... 67
End User Internet Explorer (EUIE) ... 68
Security Panel ... 69
Options Panel ... 70
Status Panel ... 71
Troubleshooting AppLock ... 72
Battery ... 15
Bluetooth ... 18
Bluetooth Devices ... 75
Discover ... 76

Bluetooth Device Menu ... 77
Bluetooth Device Properties ... 78
Settings ... 79
Turn Off Bluetooth Button ... 79
Report when connection lost ... 79
Report when reconnected ... 80
Report failure to reconnect ... 80
Computer is connectable ... 80
Computer is discoverable ... 80
Prompt if devices request to pair ... 80
Continuous search ... 81
Computer friendly name ... 81
About ... 82
Using Bluetooth ... 83
Initial Use ... 83
Subsequent Use ... 84
Bluetooth Indicators ... 85
Bluetooth Barcode Reader Setup ... 86
Introduction ... 86
MX9 with Label ... 87
MX9 without Label ... 88
Bluetooth Beep and LED Indications ... 89
Easy Pairing and Auto-Reconnect ... 89
Certificates ... 90
Data Collection Wedge ... 91
Barcode Readers ... 92
Data Processing Overview ... 93
Factory Default Settings ... 94
Main Tab ... 95
COM1 Tab ... 96
Power on Pin 9 ... 96
Notification Tab ... 97
Internal Scanner Sound ... 97
Vibration ... 97
Data Options Tab ... 98
Enable Code ID ... 99
Buttons ... 100
Data Options - Symbology Settings ... 101
Advanced Button ... 102
Clear Button ... 103

Enable, Min, Max ... 103
Strip Leading/Trailing Control ... 104
Barcode Data Match List ... 105
Barcode Data Match Edit Buttons ... 105
Match List Rules ... 106
Add Prefix/Suffix Control ... 107
Symbologies ... 108
Custom AIM IDs ... 108
Codabar - Advanced Properties ... 109
Code11 - Advanced Properties ... 110
Code39 - Advanced Properties ... 111
Interleaved 2 of 5 - Advanced Properties ... 112
MSI - Advanced Properties ... 113
Custom Code IDs - Symbol ... 114
HHP Custom IDs ... 115
Codabar - Advanced Properties ... 117
Code11 - Advanced Properties ... 118
Code39 - Advanced Properties ... 119
EAN8 - Advanced Properties ... 120
EAN13 - Advanced Properties ... 121
Interleaved 2 of 5 - Advanced Properties ... 122
Mesa - Advanced Properties ... 123
MSI - Advanced Properties ... 124
OCR Properties - Advanced ... 125
Planet - Advanced Properties ... 126
Posicode - Advanced Properties ... 127
Telepen - Advanced Properties ... 128
UPCA- Advanced Properties ... 129
UPCE0- Advanced Properties ... 130
UPCE1- Advanced Properties ... 131
Ctrl Char Mapping ... 132
Translate All ... 132
Parameters ... 133
Custom Identifiers ... 134
Parameters ... 135
Buttons ... 135
Control Code Replacement Examples ... 136
Barcode Processing Examples ... 137
HHP Properties ... 138
Centering ... 139

DecodeMode 139
LinearRange 140
AimTimer 140
LeaveLightsOn 140
About Tab 141
Length Based Barcode Stripping 142
Date / Time 143
Dialing 144
Display 144
Background 145
Appearance 146
Backlight 146
Input Panel 148
Internet Options 149
Keyboard 152
KeyMap 153
KeyMap Tab 154
LaunchApp Tab 156
RunCmd Tab 157
Mixer 158
Output panel 159
Input Panel 159
Mouse 160
Network and Dialup Options 161
Network Capture 163
Netlog 163
NDISlog 165
Options 166
Communication 166
Enable TCP/IP Version 6 166
Allow Remote Desktop Autologon 166
Autolaunch TimeSync 167
Misc 168
CapsLock 168
Touch Screen Disable 168
Enable Keypad Backlight 168
Status Popup 169
Owner 170
Password 172
PC Connection 174

Peripherals ... 175
Heaters ... 175
Flashlight ... 176
GPS ... 177
Power ... 178
Regional and Language Settings ... 180
Registry ... 182
Remove Programs ... 183
Stylus ... 184
System ... 184
General Tab ... 185
Memory Tab ... 186
Device Name Tab ... 186
Copyrights Tab ... 187
Terminal Server Client Licenses ... 188
Volume and Sounds ... 189
Good Scan and Bad Scan Sounds ... 190
WiFi Control Panel ... 191
WWAN ... 191
Connection ... 192
Network ... 192
TCP/IP ... 193
Autoconnect ... 194
Admin ... 194
About ... 195
Reflash the MX9 ... 196
Introduction ... 196
Preparation ... 196
Procedure ... 196
Reflash Troubleshooting ... 197
Battery State and OS Upgrade ... 197
Troubleshooting ... 197
Wireless Network Configuration ... 198
Important Notes ... 199
Summit Client Utility ... 199
Help ... 199
Summit Tray Icon ... 200
Wireless Zero Config Utility and the Summit Radio ... 201
Main Tab ... 202

Admin Login ... 203
Auto Profile ... 204
Profile Tab ... 205
Using the Scan Feature ... 206
Profile Parameters ... 207
IMPORTANT ... 207
Profile ... 207
SSID ... 207
Client Name ... 207
Power Save ... 207
Tx Power ... 208
Bit Rate ... 208
Radio Mode ... 209
Auth Type ... 210
EAP Type ... 210
Encryption ... 211
Status Tab ... 212
Diags Tab ... 213
Global Tab ... 214
Global Parameters ... 214
IMPORTANT ... 214
Roam Trigger ... 215
Roam Delta ... 215
Roam Period ... 216
BG Channel Set ... 216
DFS Channels ... 217
Aggressive Scan ... 217
CCX Features ... 217
WMM ... 218
Auth Server ... 218
TX Diversity ... 218
RX Diversity ... 219
Frag Thresh ... 219
RTS Thresh ... 220
LED ... 220
Tray Icon ... 220
Hide Password ... 221
Admin Password ... 221
Auth Timeout ... 221
Certs Path ... 222

Ping Payload ... 222
Ping Timeout ms ... 222
Ping Delay ms ... 222
Sign-On vs. Stored Credentials ... 223
How to: Use Stored Credentials ... 223
How to: Use Sign On Screen ... 224
Windows Certificate Store vs. Certs Path ... 225
User Certificates ... 225
Root CA Certificates ... 225
Configuring the Profile ... 227
No Security ... 228
WEP ... 229
LEAP ... 230
PEAP/MSCHAP ... 231
PEAP/GTC ... 233
WPA/LEAP ... 235
EAP-FAST ... 237
EAP-TLS ... 238
WPA PSK ... 241
Certificates ... 242
Generating a Root CA Certificate ... 242
Installing a Root CA Certificate ... 245
Generating a User Certificate ... 247
Installing a User Certificate ... 253
Peripherals / Accessories ... 256
Carry Case ... 256
Hand Strap ... 256
Holster ... 256
Stylus ... 256
Trigger Handle ... 256
Battery Multi-charger ... 257
Status Indicators ... 257
Docking Cradles ... 258
Desktop Cradle ... 258
Vehicle Cradle ... 258
KeyMaps ... 259
Introduction ... 259
MX9 62-Key Keypad ... 260
KeyMaps 62-Key 5250 Overlay ... 266

MX9 38-key Keypad 267
Technical Specifications 272
MX9 272
Dimensions and Weight 273
Environmental Specifications 273
Main Battery Technical Specifications 274
Wireless Radio 274
Bluetooth System Compatibility 275
WWAN Radio 275
AC/DC Wall Adapter 275
GPS Receiver Technical Specifications 276
Frequency Band 276
Serial Interface 276
Accuracy 276
Protocol 276
AppLock Error Messages 277
Hat Encoding 284
Revision History 285
Index 286

Introduction

The LXE® MX9 is a ruggedized handheld computer targeted for indoor and outdoor use. It is powered by a lightweight main battery that can be removed and replaced without the need for special tools.

MX9 wireless connectivity is secured by user-configured encryption and authentication protocols. The MX9 has an integrated keyboard, outdoor readable touch display, a tethered stylus, Microsoft® Windows® CE® 5.0 operating system, and many wireless connection options.

The keypad is available in a 62-key or 38-key configuration. The 62-key keypad is also available in an IBM 5250 configuration.

Barcode reader options are: an imager or laser scanner integrated in the MX9, or a handheld scanner tethered to the port at the base of the MX9, Bluetooth mobile barcode imagers and scanners, or the LXE Bluetooth ring scanner / ring imager.

Wireless network connection can be accomplished using a Summit WLAN 802.11 radio, WWAN, and Bluetooth.

Desk and vehicle cradles, a trigger handle or handstrap, holsters with shoulder straps or belts, clear covers for cases and holsters, Bluetooth scanners and printer, standard and low temperature batteries, and battery chargers are among the many accessories available for the MX9.

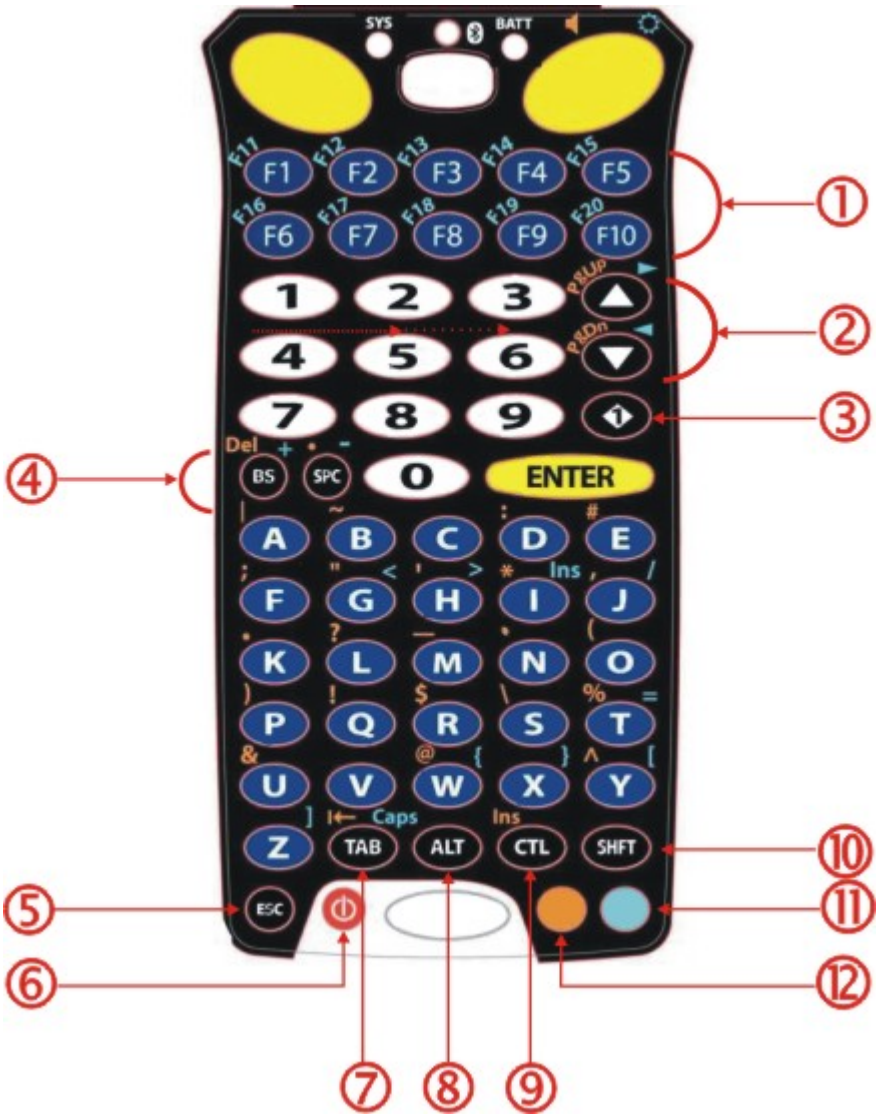
Components

Front

1. Microphone
2. Touch screen
3. Speaker
4. Scan buttons
5. Enter key
6. Scanner status LED
7. Power key

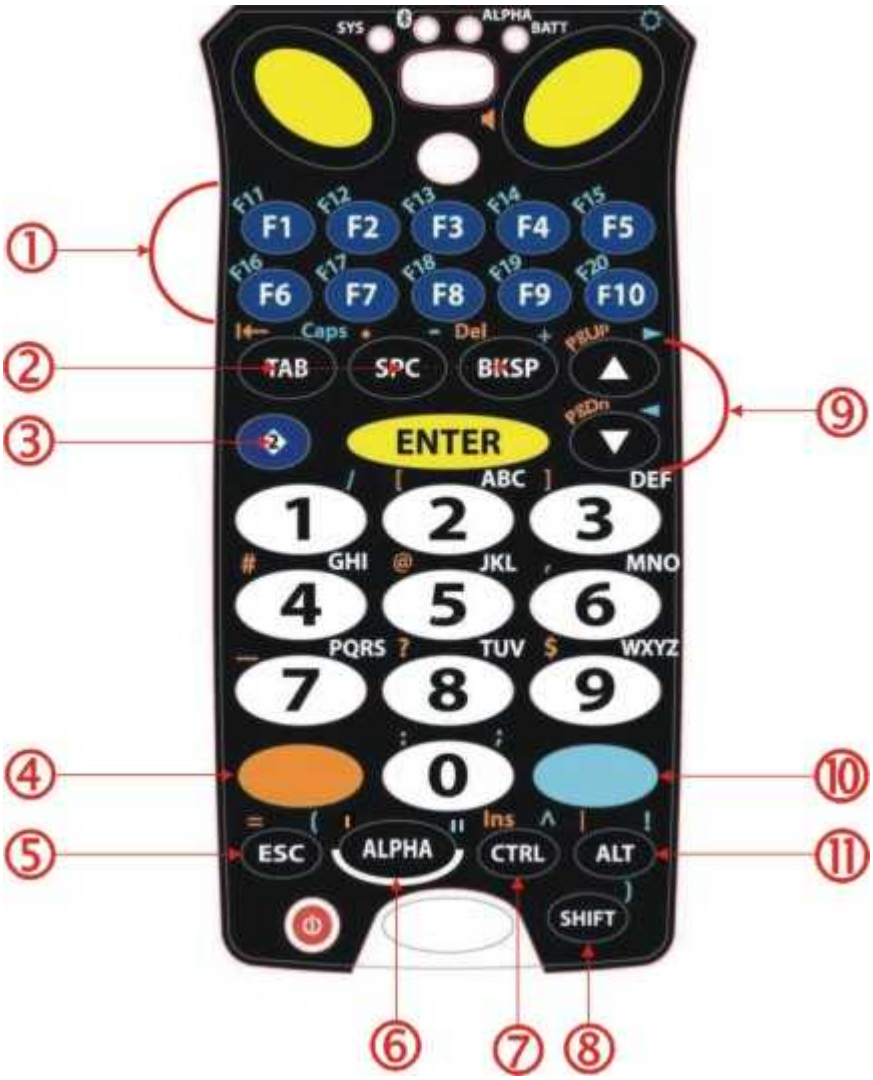
Note: The above list is the same on the 38 key MX9. Special keys are listed below.

Special Purpose Keys



1. Function Keys
2. Cursor up and down Keys
3. Diamond 1 key
4. Backspace [BS] key and Space [SPC] key
5. Escape [ESC] key
6. Power key
7. Tab key
8. Alt key
9. Control [CTL] key
10. Shift [SHFT] key
11. Blue key
12. Orange key

Special Purpose Keys - 38 Key



1. Function keys
2. Tab | Space | Backspace keys
3. Diamond 2 key
4. Orange key
5. Escape [ESC] key
6. Alpha key
7. Control [CTRL] key
8. Shift [SHIFT] key
9. Cursor up and down keys
10. Blue key
11. Alt key

Top

Barcode reader Imager aperture

Barcode reader Scanner aperture

Bottom

Input / Output Connector

Tethered boot cover (covers I/O connector) not shown

Back

Battery Bay

1. Battery Terminals
2. Battery Bay
3. Battery Bay Access Tab

Trigger Handle

Trigger handle attach points

1. Upper
2. Lower

1. Trigger
2. Tether attach point

Stylus storage bay in handle

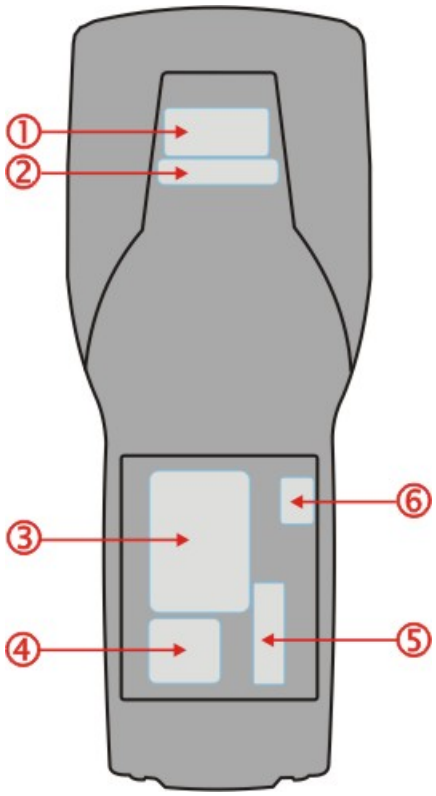
Handstrap

1. Handstrap
2. Handstrap Base
3. Stylus

1. Attach - Upper Handstrap Base
2. Attach - Lower Handstrap Base

1. Handstrap connector, upper
2. Stylus holder on Handstrap
3. Handstrap connector, lower

Label Locations



1. Laser Warning Label
2. Bluetooth Label
3. Product Identification Label
4. Java Label (if installed)
5. Windows CE License Label
6. Tamper Proof Label

The tamper-proof label covers the top right screw in the battery bay. The label states "Warranty void if removed or damaged". The battery pack will not deface the label as the battery pack does not touch the label.

Device with Summit Radio

Hardware

System Hardware

Central Processing Unit

The **CPU**[1] is a 806 MHz Marvell PXA-320 CPU. The operating system is Microsoft Windows CE 5.0. The OS image is stored on an internal SD flash card and is loaded into DRAM for execution.

Turbo mode switching is supported and turned on by default.

The MX9 supports the following I/O components of the core logic:

- One serial port (DTE) with appropriate power for a WAN radio
- One serial port (DTE) for an integrated laser decoder with RI
- USB 1.1 Host (capable) with power (5V @ 500mA)
- One SSP port (capable)
- One SDIO port for I/O expansion (capable)
- One SIM port for WAN
- One serial port (DTE) for interface with GPS receiver chip
- Non-decoding imager

System Memory

The MX9 supports 128 MB on-board RAM and 128 MB on-board Flash. Operating system and boot loader software image update is supported via expansion card and remote management via radio.

Internal flash is used for boot loader code and system low-level diagnostics code. Bootloader code is validated at system startup. The UUID required by CE 5.0 is stored in the boot flash. A second copy of the bootloader code is stored on the internal SD Flash drive, so that if a damaged bootloader is detected, it may be re-flashed correctly.

Internal SD Memory Card

The MX9 has one SD card interface for storage of operating system and program code, as well as persistent storage.

The internal SD flash card appears to the OS as a folder. This allows the contents to be manipulated via the standard Windows CE interface.

[1] Central Processing Unit

Video Subsystem

The touch screen display supports **QVGA**[1] and 16 bit color depth, and is readable indoors or outdoors even in direct sunlight.

The display is **Transflective**[2] **Active matrix**[3] **TFT**[4] and has an **LED**[5] backlight.

A tethered stylus is included. The touch screen surface can be activated with the stylus or a gloved or bare finger.

The Cold Storage option includes a touch screen heater and a scan aperture heater to eliminate condensation. The heaters can be enabled or disabled by the user. Once enabled, the heaters will turn on whenever the ambient temperature warrants, for example, when moving into and out of freezers or refrigerated buildings.

Power Supply

The MX9 uses one of two batteries for operation. A Lithium-Ion (Li-Ion) standard battery has a 2400 mAh capacity. Low temperature Lithium-Ion (Li-Ion) batteries have a 2100 mAh capacity.

Input/Output Connector

A single external connector at the base of the MX9 provides the following signals:

- USB Host and USB Client
- RS-232 with support for powering a tethered device (e.g. scanner or mager)
- Audio in and out for headset
- Power input
- Ethernet (only accessible when MX9 is secured in a cradle's docking bay)

The MX9 cables are designed to be securely connected to this port. This port is also used to connect the MX9 to the docking bay connector in cradles.

A tethered protective cap is provided to cover the external port when it is not in use.

---

[1] Quarter Video Graphics Array (320 by 240 pixels; 1.33:1 aspect ratio).

[2] Transflective LCDs are a mixture of the technology found in Reflective LCDs and Transmissive LCDs. The rear polarizer has partial reflectivity and is combined with a backlight for use in all types of lighting conditions. In sufficient lighting, the backlight can be left off to conserve power. The backlight can be turned on to provide a bright display in low-light areas. Transflective LCDs do not “wash out” when operated in direct sunlight.

[3] A flat panel display, most commonly using TFT technology, which is refreshed more frequently than a passive matrix display. An active matrix display uses a transistor to control each pixel.

[4] Thin Film Transistor

[5] Light Emitting Diode. A diode that lights up when a voltage is applied to it. The diode is made of a substance that illuminates when electricity passes through it.

Bluetooth

The MX9 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains network connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections to or from the MX9. However, the MX9 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the MX9 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user's passcode.

The Bluetooth hardware in the MX9 allows simultaneous connection to two LXE Bluetooth peripherals using the LXEZ Pairing control panel application.

Bluetooth device connection supported on the MX9 includes:

- Bluetooth scanners / imagers
- Zebra printer models
- LXE Back of Hand Scanner

Barcode data captured by the Bluetooth scanner is manipulated by the settings in the MX9 Data Collection Wedge Properties control panel.

Multiple beeps may be heard during a barcode scan using a mobile Bluetooth scanner; beeps from the mobile Bluetooth scanner as the barcode data is accepted/rejected, and other beeps from the MX9 during final barcode data manipulation.

Audio Support

All Microsoft-supplied audio codecs are included in the OS image. The hardware codecs, the input and output analog voice circuitry and the system design are designed to support voice applications using a headset accessory cable.

802.11 b/g and a/b/g Wireless Client

The MX9 has an LXE 802.11x network card that supports diversity with two internal antennas. The CPU board does not allow hot swapping the network card. Power management on the network card is set to static dynamic control.

WEP, WPA and LEAP are supported.

External Input/Output Port

A single external connector at the base of the MX9 provides the following signals:

- USB Host and USB Client
- RS-232 with support for powering a tethered device (e.g. scanner or imager)
- Audio in and out for headset
- Power input
- Ethernet (accessible when MX9 is secured in a cradle's docking bay)

The MX9 cables are designed to be securely connected to this port. This port is used to connect the MX9 to the docking bay connector in cradles.

A tethered protective cap is provided to cover the external port when it is not in use.

COM Ports

COM Port	Used By	Default Power Setting	Communication Default
1	External serial	On	9600 baud, 8 bits, no parity, 1 stop bit
2	Bluetooth	On	9600 baud, 8 bits, no parity, 1 stop bit
3	WWAN	Off	9600 baud, 8 bits, no parity, 1 stop bit
4	Integrated Barcode Reader	On	9600 baud, 8 bits, no parity, 1 stop bit
5	GPS	Off	9600 baud, 8 bits, no parity, 1 stop bit (Default baud rate is 4800 for NMEA communications)

Keypads

The MX9 keypad is either a 62-key full alphanumeric keypad or 38-key numeric-alpha.

The 62 key keypad has an ANSI or a 5250 overlay.

The keypad backlight default setting is to follow the display backlight setting until it is changed by the user.

Keymaps

Modifier Keys

The modifier keys are located at the bottom of the keypad. The modifier keys are orange and blue.

A modifier key pressed after itself toggles that modifier mode off.

A modifier keypress cancels the other modifier's active state. Then the state of the modifier key that was pressed last becomes active. For example, if the Orange modifier state is active (MX9 is currently in Orange mode), pressing the Blue key cancels Orange mode and sets Blue mode active.

Once a modifier key is pressed, the modifier map state continues until another key is pressed.

The Orange and Blue keys do not need to be held down while another key is pressed.

Modifier keys do not auto-repeat.

Expansion Slots

- Summit radio card
- SIM card
- SD card

The expansion slots in the MX9 are accessible via the hatch. The hatch can be opened using a standard size screwdriver. When the hatch is opened, the MX9 automatically shuts down.

SD card configurations in 512MB, 1GB and 4GB are available from LXE.

Note: It is good practice to save your changes then perform an orderly shutdown to preserve RAM contents before opening the hatch.

Power Key Functions

The Power key is located at the bottom of the keypad, next to the Scanner LED.

The Power On/Off key is a momentary contact.

Behavior is as follows:

When the MX9 is in ...	**Pressing the Power key ...**
Off mode	boots the unit and sets it to the On mode
On mode	sets the unit in Suspend mode
Suspend mode	sets the unit in On mode
Critical Suspend mode	has no effect
Backlight off mode	sets the unit in Suspend mode
Display off mode	sets the unit in Suspend mode

Status LEDs

Several **LED**[1]s are located on the front of the MX9 above the integrated speaker. They are:

- **System Status LED** indicates power management status.
- **Battery Charging Status LED** indicates main battery charging status.
- **Alpha Mode Status LED** applies to the 38-key keypad only.
- **Bluetooth Status LED** applies to Bluetooth client functions.

System Status LED

Blinking Red	Battery power fail; critical suspend
Solid Red	Main battery low
Blinking Green	Display turned off
Yellow / Amber	Initial few seconds when Power key is pressed

Battery Charging Status LED

Off	No battery, no AC power, battery pack not plugged in or no AC power applied
Flashing Red	Fault, battery pack fault or failure
Yellow / Amber	Standby, battery pack temperature out of range
Red	Charging, battery pack charging (icon on touchscreen)
Green	Charged, battery pack fully charged. Connected to external power.

Alpha mode Status LED

- Green when in alpha mode, 38-key keypad only.

Bluetooth Status LED

Blinking slowly	Bluetooth is active but not connected to a device.
Blinking medium	Bluetooth is paired and connected to a device.
Blinking fast	Bluetooth is discovering other Bluetooth devices.
Unlit	Bluetooth hardware has been turned off or does not exist in the MX9.

[1]Light Emitting Diode. A diode that lights up when a voltage is applied to it. The diode is made of a substance that illuminates when electricity passes through it.

Scanner Status LED

The integrated scanner, and imager, Scan Status LED is centered below the MX9 keypad, next to the Power button.

- Steady green indicates a good scan
- Steady red indicates a scan is in progress
- Steady yellow/amber indicates parameter changes are being written to the integrated scanner/imager engine

The Scan Status LED illuminates when a Scan button on the MX9 is depressed (scan in progress), or the trigger on the attached handle is pressed (scan in progress), or when the scanner/imager engine parameters have been changed and the changes are being saved (writing to scan engine). While the changes are being saved, the scanner/imager is inoperable.

- The MX9 Scan Status LED does not illuminate when the Scan button is pressed on a scanner cabled to the MX9 or cabled to an MX9 cradle communication port. The Scan LED on the cabled scanner/imager illuminates.
- The MX9 Scan Status LED does not illuminate when the Scan button is pressed on a wireless Bluetooth mobile scanner paired with the MX9. The Scan LED on the wireless Bluetooth mobile scanner/imager illuminates.

Note: A scanned barcode can be accepted as a good scan or a bad scan by the MX9 barcode decoder (as configured). The appropriate audible or tactile indicator is activated.

Note: The result of the host processing (as configured) of the good scan barcode data can indicate either accept or reject. If rejected, a bad scan indicator is activated if the host process has been configured to indicate audible or tactile accept or reject.

Vibrate Indicator

The MX9 has a vibration motor.

It is user-configurable to vibrate on a good scan, bad scan, or via an API call. The vibrations from this motor are detectable under the handstrap at the rear of non-handle units or through the trigger handle when a trigger handle is installed.

Three vibration duration settings are provided for both good and bad scan. The settings can be assigned using tab. The default setting for both good scan and bad scan is Off.

Cold Storage

When the MX9 has been configured as a cold storage or low temperature device, a snowflake icon is visible under the touch screen next to the product name.

The MX9, with its special low temperature battery and condensation controlling heaters is designed specifically for use in freezers and refrigerator environments including transitioning between the two.

Technical Specifications

Heating Elements

Heating elements activate when ambient temperature drops below 0°C (32°F). LXE recommends using the stylus *only* when performing screen touch functions on the display when the temperature drops below freezing.

There may be some condensation as the MX9 moves in and out of cold storage areas. The condensation on the touchscreen and the scan aperture quickly dissipates.

Although no user interaction is required to enable the heating elements, the automatically controlled heating elements can be enabled and disabled using the options in the Peripherals control panel.

Cables

Note: Do not connect or disconnect cables in a Hazardous location.

- I/O port to USB host and power pigtail for external power
- I/O port to USB client and power pigtail for external power
- I/O port to RS-232 with power
- I/O port to RS-232 without power
- I/O port to 4-wire headset connector with quick-disconnect capability.
- Ethernet Category 5 cable, 6ft / 2m. *(only the Cradle has an RJ-45 port for the Ethernet CatV cable)*

Cable connections are covered in more detail in the MX9 User Guide.

Scanners and Imagers

Note: The maximum number of communication ports from which the Data Collection Wedge can simultaneously support input is three.

Integrated Barcode Decoders

The MX9 may have any of the following barcode readers built in (integrated) and protected by the hatch:

- SE955 standard range laser scanner engine (barcode decoding only)
- SE1524 Lorax laser scanner engine (barcode decoding only)
- HHP 5300SF laser imager engine (nondecoding)

A **scan aperture**[1] heater is implemented for low temperature environments.

Tethered Barcode Decoders

The external serial port at the base of the MX9 is used to connect (via serial tether) the LXE 8500-series Fuzzy Logic laser scanners as needed.

Bluetooth Client Barcode Decoders

The Bluetooth Module in the MX9 can accept data from the following LXE Bluetooth barcode readers:

- 8650 Wearable (Back of Hand) Bluetooth module with ring decoders, either laser scanner or 1D/2D imager.
- 8700 Bluetooth Imager
- 8810 Bluetooth Fuzzy Logic laser scanner
- 8820 Bluetooth Lorax laser scanner

GPS Module

The default setting for GPS is Off.

GPS (Global Positioning System) is a U.S. space-based radio navigation system that provides reliable positioning, navigation, and timing services on a continuous basis. The primary function of the embedded GPS module is to provide worldwide location to applications which are running on the MX9.

GPS presence is displayed on the Peripherals control panel. Using the GPS tab, GPS power can be toggled on or off only when a GPS is installed.

Technical Specifications

[1] A narrow opening, usually covered by glass or high-impact clear plastic, that lets laser beams pass through.

Power

Main Battery

Note: New batteries must be fully charged prior to use.

The MX9 is designed to work with a replaceable 2400 mAh Lithium-Ion (Li-Ion) battery pack from LXE. Under normal conditions it should last approximately eight hours before requiring a recharge.

MX9 low temperature 2100 mAh Lithium-Ion (Li-Ion) batteries (designed for freezer environments and with a blue label) have an average use time of 4 hours before requiring a recharge.

During very heavy scanning or wireless transmitter use, the operating time of the battery may be less.

A depleted battery can be hot-swapped with a fully charged battery after the MX9 is placed in Suspend mode. A battery charge level indicator on the taskbar displays the present battery charge to within 15% of the current battery capacity.

HazLoc versions of the MX9 require a screwdriver to remove the plate covering the battery release mechanism.

When the MX9 is docked in a powered cradle, the battery in the MX9 is recharged through the cradle connector in the docking bay. An extra Li-Ion battery pack can be recharged in a powered desktop cradle. The battery is fully recharged in a powered cradle in less than 4 hours. The MX9 can be Off, in use or in Suspend Mode while the battery is recharging.

Note: When the main battery and backup power system are fully depleted, the MX9 turns off. The operating system reverts to the last saved registry settings when a fully powered battery is inserted and the MX9 is turned on.

See Also: Battery Technical Specifications

External Power Supplies

External power supplies are available for the following:

- any I/O cable with a power connector
- desk cradle
- vehicle cradle
- car power adapter (CLA)
- Battery multi-charger

The indoor power supplies (e.g. AC/DC Adapters) use IEC320-C 14 AC power connectors.

The car power adapter uses the cigarette lighter adapter (CLA) and is powered by the vehicle's automotive 12V battery. The adapter power supply converts the input voltage into a voltage suitable to power the MX9 and charge the unit's internal backup battery.

The vehicle mount cradle uses a 36V, 24-60V or 70-150V DC-DC power supply.

Note: The MX9 and desk cradle and multi-charger use the same external power supply.

AC/DC 15V Power Supply

The MX9 receives AC/DC power from the AC/DC (15 VDC - 4 Amp - 60 Watt) Power Supply. The MX9 external power connection is part of the serial cable assembly and the USB cable assembly.

The AC/DC Power Supply is connected to a wall outlet then to the power cable secured to the base of the MX9.

Note: The LXE-approved AC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.

The indoor power supply has a IEC320-C 14 AC power connector.

When the power supply is receiving AC/DC power from the wall outlet, an LED on the power supply illuminates green. The green LED indicates the power supply is ready for use.

This AC/DC power supply is designated for:

- the MX9 I/O port multi-cables
- the MX9 desktop cradle
- the MX9 battery multi-charger

There are specific DC/DC power supply adapters for the MX9 vehicle cradle; do not use any other power supply with the vehicle cradle.

Car Power Adapter

The MX9 Car Power Adapter is a self-contained unit. The cable has one and a half feet of coiled cord and one and a half feet of straight cord. The coiled portion is on the end of the adapter. An LED on the adapter illuminates when the car power adapter is receiving vehicle input power.

The cigarette lighter adapter contains a power supply which converts the vehicle's nominal 12V to 15V, a voltage suitable to power the MX9 and charge the MX9 battery.

One end consists of a plug compatible with a standard vehicle cigarette lighter adapter (**CLA**[1]). The Car Power Adapter has a standard size CLA plug that uses center positive (+12V) and sleeve ground. A replaceable fuse is provided on the input side.

The other end of the three foot cable connects to the MX9 36-pin I/O port. It has a security latch for stability when connected to the Car Power Adapter cable.

Replace CLA Fuse

Equipment needed: 5A fuse of the same size and amperage.

Remove the CLA from the cigarette lighter outlet on the vehicle.

Disconnect the cable from the MX9.

Unscrew the tip of the adapter end.

Replace the blown fuse with a fuse of the same rating and size.

Screw the tip back on to the adapter end, replacing any previously removed parts in the order in which they were removed.

Troubleshooting: Upon reassembling the cigarette lighter adapter with the new fuse, and plugging it into the cigarette lighter port on the vehicle -- if the **LED**[2] on the CLA does not illuminate green, there may be a problem with your vehicle power source.

---

[1] Cigarette Lighter Adapter. Refers to the cigarette lighter port found in most automobiles.
[2] Light Emitting Diode. A diode that lights up when a voltage is applied to it. The diode is made of a substance that illuminates when electricity passes through it.

Power Modes

On

When in the On state, the display (touchscreen) is on. The keyboard, touchscreen and all peripherals function normally. The display backlight is on until the User Idle timer expires. The display does not turn off until the System Idle timer expires.

Only interrupts classified as User Activity events will keep the unit in the On state.

MX9 User Activity Events are:

Note: These items are not configurable selections.

- Any key on the keypad except the Power key
- Incoming data through scanner port
- Touch screen tap
- Trigger pull

The user is presented with a Power applet in the Control Panel. One tab in the applet, Schemes, is designated for the power management timeouts. This tab displays three transition states, User Idle, System Idle and Suspend.

Additionally, the OS provides a Backlight tab on the Display control panel. he Backlight tab allows the user to select the same timeout ranges provided by the User Idle scheme timers. Any changes on the Display | Backlight tab will also change the Power | Schemes | User Idle timer, and vice-versa.

The backlight for the keypad (if enabled) will always follow the display backlight.

User Idle

When transitioning from the On power state to the User Idle power state, the keypad backlight (if enabled) is dimmed and the display backlight is dimmed. User Activity Events listed below will transition the system back to the On state.

User Idle timers are set using Start | Settings | Control Panel | Power | Schemes tab.

Only interrupts classified as System Activity events will keep the MX9 awake in this state until a deliberate user action to put the unit into Suspend or power Off occurs. An event must be specifically coded to wake up from this state.

The following User Activity events DO transition the unit from the User Idle state to On state:

Note: These items are not configurable selections

- Any key on the keypad except the Power key
- Incoming data through the scanner port[1]
- Touch screen tap
- Unit docked in powered cradle
- Trigger pull
- Incoming Bluetooth connection or data on the virtual COM port
- Connection of USB Device to host port

[1] The scanner port is defined as a software (SW) port. Any hardware (HW) device that sends data to the software (SW) defined scanner port will transition the unit from User Idle to On.

The following events DO NOT wake the unit from the User Idle state or reset the timers:

- COM1 CTS
- Serial connection
- USB client connection to a host PC
- Power key press (transitions to Suspend)

Example: Bluetooth Voice will not transition the unit from User Idle to On. Bluetooth Scan data will transition the unit to On as it sends the data to the scanner port.

System Idle

After transitioning to the User Idle power state, the timer is started for the transition to System Idle. When this timer expires without any further user activity, the keypad backlight (if enabled) is turned off and the display is turned off. Only interrupts classified as System Activity events will wake the unit from System Idle to User Idle. Any activity classified as User Activity will transition from System Idle to On.

System Idle timers are set using **Start | Settings | Control Panel | Power | Schemes** tab.

The following System Activity events DO transition the MX9 from the System Idle state to User Idle state:

Note: These items are not configurable selections.

- RF Data
- Ethernet Data
- Serial Data
- USB Data

Note: Pressing and releasing the Power key while the MX9 is in the System Idle state will cause it to transition to the Suspend state.

Suspend

The Suspend mode is entered when (1) the unit is inactive for a predetermined period of time, (2) the user taps the Power key, or (3) Start | Suspend is chosen. Inactivity means that no devices are causing interrupts to reset the power state.

The Suspend timer is set using **Start | Settings | Control Panel | Power Properties | Schemes** tab.

By default, any of the primary events listed below will wake the unit and reset the User Idle, System Idle, and Suspend timers.

When the unit wakes up, the User Idle, System Idle and the Suspend timers begin the countdown again. When any one of the above events occurs prior to the Suspend timer expiring, the timer starts the countdown again.

The first wakeup key press or touch is not sent to the operating system or running application. The first key press or touch is only used to wake up the unit and reset the timers. Once the unit has transitioned from the Suspend mode to the On mode, the unit, keyboard and touch screen function normally.

The transition to the Suspend power state occurs during the following events:

- Timeout of the User Idle, System Idle and Suspend inactivity timers.
- The Power key on the target device is pressed.
- An application program calls the Suspend function.

The MX9 will only resume from a suspended state if an interrupt occurs and the CPU has been programmed to wake when an interrupt occurs. An interrupt from any listed device transitions the OS back to the On state.

Suspend Primary Wake up Events

Wake up Events - all configurable via command line utility:

- Power key
- Touch screen
- Any integrated keypad touch
- Bluetooth connection capable
- USB client connection
- COMM CTS - Serial port handshaking - i.e. tethered scanners generate CTS which could wake up the unit
- Trigger pull (MX9 with integrated barcode decoder only)
- Internal serial port device interrupt (WAN, etc. - only devices capable of signaling an interruptible GPIO, and that have a separate power supply)
- External power applied
- Real-Time Clock (RTC) (Win32 API call CeRunAppAtTime will not work if this is turned off)
- Detection of external microphone

Wake Up Event Default Settings

Enabled	Disabled
Power key	Bluetooth connection
Touchscreen tap	COMM CTS
Integrated keypad key press	Internal serial port device IRQ
USB client connection	Push to talk on audio headset
External power applied	Detection of external microphone
Real-time clock	
Trigger handle trigger press	

Events that do NOT wake up from Suspend - these events are not available to be configured to wake the unit up from suspend

- External keyboard/mouse
- Ethernet (data or connection)
- USB Host (data or connection)
- USB client disconnection
- Serial data
- Internal Serial port handshaking (WAN, etc)
- 802.11 radio
- Docked signal (i.e. a non-powered cradle would not wake the MX9 up, but a powered cradle could be a wake up event if External Power is set to be a wake up event)
- MPF (Main Power Failure)
- Audio data
- Display data

Critical Suspend

The purpose of the Critical Suspend mode is to maintain data stored in RAM with minimum power consumption. If the Main Battery is removed, the Backup Battery is supplying power to the MX9 during Critical Suspend Mode. If Main Battery power is re-applied, the device will transition to Suspend mode. If Main Battery power is not made available before the Backup Battery is depleted, the unit enters Off Mode.

Off

The MX9 enters the Off Mode when the Main Battery and the Backup Battery are depleted or when Shutdown is selected from the Start menu.

Software

Operating System

Your MX9 operating system is Windows CE 5.0. The MX9 operating system revision is displayed on the Desktop. This is the factory default value for the Desktop Display Background.

Windows CE 5.0 Operating System

For general use instruction, please refer to commercially available Windows CE user's guides or the Windows CE on-line Help application installed with the MX9.

This segment assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the MX9 and its Windows CE environment.

General Windows CE Keyboard Shortcuts

Use the keyboard shortcuts in the chart below to navigate with the MX9 keyboard. These are standard keyboard shortcuts for Windows CE applications.

Press these keys …	**To …**
CTRL + C	Copy
CTRL + X	Cut
CTRL + V	Paste
CTRL + Z	Undo
DELETE	Delete
SHIFT with any of the arrow keys	Select more than one item in a window or on the desktop, or select text within a document.
CTRL+A	Select all.
ALT+ESC	Cycle through items in the order they were opened.
CTRL+ESC	Display the Start menu.
ALT+Underlined letter in a menu name	Display the corresponding menu.
Underlined letter in a command name on an open menu	Carry out the corresponding command.
ESC	Cancel the current task.

The touchscreen provides equivalent functionality to a mouse:

- A touch on the touchscreen is equivalent to a left mouse click.
- Many items can be moved by the “drag and drop” method, touching the desired item, moving the stylus across the screen and releasing the stylus in the desired location.
- A double stylus tap is equivalent to a double click.
- A touch and hold is equivalent to a right mouse click.

Note: Some applications may not support this right click method. Please review documentation for the application to see if it provides for right mouse click configuration.

Warmboot

A warmboot reboots the computer without erasing any registry data. Applications and data in RAM are preserved during a warmboot.

All registry configurations are automatically preserved. Any applications stored as .CAB files in the System directory and configured in the registry to persist are reinstalled on boot up by the Launch utility.

Clearing Persistent Storage / Reset to Default Settings

Use the Registry control panel to reset the MX9 to .factory defaults.

Folders Copied at Startup

The following folders are copied on startup:

- System\Desktop=> Windows\Desktop
- System\Favorites=> Windows\Favorites
- System\Fonts=> Windows\Fonts
- System\Help => Windows\Help
- System\Programs=> Windows\Programs

This function copies only the directory contents, no sub-folders.

The following folders are NOT copied on startup:

- Windows\AppMgr
- Windows\Recent
- Windows\Startup

Because copying these has no effect on the system or an incorrect effect.

Files in the Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by launch.

Saving Changes to the Registry

The MX9 saves the registry when you:

- Tap Start | Run then type Warmboot. Tap OK.
- Perform a Suspend / Resume function (by pressing the Pwr key and then pressing it again).

The registry save process takes 0 – 3 seconds. If nothing has been changed, nothing is saved (e.g. 0 seconds)

The registry is automatically saved every 10 seconds if anything has changed. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel applet (e.g. Date/Time) parameters are changed by the user and a warm boot was not performed afterward.

Software Load

The software loaded on the mobile computer consists of Windows CE 5.0 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

- Full Operating System License: Includes all operating system components, including Windows CE 5.0 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touchscreen input, window management, and common controls.
- Network and Device Drivers
- Bluetooth (Optional)

Note: Contact your LXE representative for software updates and CAB files as they are released by LXE.

Software Applications

The following applications are included:

- WordPad (was PocketWord in previous versions of Windows CE)
- DCWedge (barcode result manipulation)
- ActiveSync
- Transcriber
- Internet Explorer
- Word Viewer
- Excel Viewer
- PDF Viewer
- Image Viewer

Note that the viewer applications allow viewing documents, but not editing them.

Bluetooth (Optional)

Only installed on a Bluetooth equipped MX9. The System Administrator can Discover and Pair targeted Bluetooth devices for each MX9. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly name for each MX9.

The Bluetooth control panel can be accessed by tapping **Start | Settings | Control Panel | Bluetooth** or by doubletapping the Bluetooth icon in the taskbar or on the desktop.

LXE RFTerm (Optional)

Installed by LXE. The application can be accessed by clicking **Start | Programs | RFTerm**.

MX9 Utilities

The following files are pre-loaded by LXE.

LAUNCH.EXE

Launch works in coordination with registry settings to allow drivers or applications to be loaded automatically into DRAM at system startup. Registry settings control what gets launched; see the App Note for information on these settings. For examples, you can look at the registry key

HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist

Launch will execute .CAB files, .BAT files, or .EXE files.

App Note

All applications to be installed into persistent memory must be in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and are copied to the CE device using ActiveSync, or using a Compact Flash ATA card. The CAB files are copied from ATA or using ActiveSync Explore into the folder System, which is the persistent storage virtual drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist, as follows. The main subkey is any text, and is a description of the file. Then 3 mandatory values are added:

FileName is the name of the CAB file, with the path (usually \System).

Installed is a DWORD value of 0, which changes to 1 once auto-launch installs the file.

FileCheck is the name of a file to look for to determine if the CAB file is installed. This will be the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

There are three optional fields that may be added:

Order is used to force a sequence of events. Order=0 is first, and Order=99 is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence.

Delay is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to 0 if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.

PCMCIA is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the PCMCIA field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of 0 means the slot is not powered on. The default values for the default radio drivers (listed below) is 1, meaning one second elapses between the CAB file loading and the slot powering up.

The auto-launch process proceeds as follows:

- The launch utility opens the registry database and reads the list of CAB files to auto-launch.
- First it looks for FileName to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the Installed flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it.
- If the Installed flag is set, auto-launch looks for the FileCheck file. If it is present, the CAB file is installed, and that registry entry is complete. If the FileCheck file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file.
- Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.

- To force execution every time (for example, for AUTOEXEC.BAT), use a FileCheck of “dummy”, which will never be found, forcing the item to execute.
- For persist keys specifying .EXE or .BAT files, the executing process is started, and then Launch will continue, leaving the loading process to run independently. For other persist keys (including .CAB files), Launch will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.
- Note that the auto-launch process can also launch batch files (*.BAT), executable files (*.EXE), registry setting files (*.REG), or sound files (*.WAV). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Registry information is already in the default image for the following:

Note: Registry entries may vary depending on software revision level and options ordered with the MX9.

LAUNCH.EXE and Persistent Storage

If any of the following directories are created in the \SYSTEM folder, Launch automatically copies all of the files in these directories to the respective folder on the flash drive:

- AppMgr
- Desktop
- Favorites
- Fonts
- Help
- Programs
- Recent

Note: Files in the Startup folder are executed, but only from \System\Startup. They are not copied to another directory.

REGEDIT.EXE

Registry Editor – LXE recommends caution when editing the Registry and also recommends making a backup copy of the registry before changes are made.

REGLOAD.EXE

Double-tapping a registry settings file (e.g. REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

REGDUMP.EXE

Registry dump – Saves a copy of the registry as a text file. The file, REG.TXT, is located in the root folder.

Note: The REG.TXT file is not saved in persistent storage. To use the REG.TXT file as a reference in the even of a coldboot, LXE recommends copying the file to the \SYSTEM directory on the MX9 or storing a copy of the file on a PC.

WAVPLAY.EXE

Double tapping a sound file (e.g. WAV) causes WavPlay to open the file and run it in the background.

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap Start | Run and type **prtscrn** and tap OK, or press Enter. There is a 10 second delay before the screen print is made. The device beeps and screen captured file (*scrnnnn*.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

API Calls

See Also: LXE CE API Programming Guide

The LXE CE API Programming Guide documents only the LXE-specific API calls for the MX9. It is intended as an addition to the standard Microsoft Windows CE API documentation. Details of many of the calls in the LXE guide may be found in Microsoft's documentation.

The APIs documented in the programming guide are included in the file LXEAPI.DLL, which is in the standard Windows CE image on the MX9.

For ease of software development, the files LXEAPI.H and LXEAPI.LIB are available on the accessories CD, which are the C/C++ include files and the link library for the DLL, respectively.

A full SDK is now included for Microsoft Embedded Visual C++ 4.0 (which is available free on the Microsoft website).

Access Files on the Flash Card

Click the **My Device** icon on the Desktop then click the System icon.

A flash card is used for permanent storage of the MX9 drivers, CAB files and utilities. It is also used for registry content back up.

CAB files, when executed, are not deleted.

Note: Always perform a warmboot (Start / Settings / Control Panel / Registry) when exchanging one flash card for another.

Desktop Icons

For general use instruction, please refer to commercially available Windows CE user's guides or the Windows on-line Help application installed in the mobile device.

The MX9 Desktop appearance is similar to that of a desktop PC running Windows 2000 or XP.

At a minimum, it has the following icons that can be double tapped with the stylus to access My Computer, Internet Explorer, and the Recycle Bin.

At the bottom of the screen is the Start button. Tapping the Start Button causes the Start Menu to pop up. It contains the standard Windows menu options: Programs, Favorites, Documents, Settings, Help, and Run.

Desktop Icon	Function
My Device	Access files and programs.
Recycle Bin	Storage for files that are to be deleted.
Bluetooth	Discover and then pair with nearby discoverable Bluetooth devices.
My Documents	Storage for downloaded files / applications.
Internet Explorer	Connect to the Internet/intranet (requires radio card and Internet Service Provider – ISP enrollment is not available from LXE).
Summit Client Utility	Used for accessing the appropriate wireless configuration, SCU (Summit Client Utility).
LXE RFTerm	RFTerm is an optional terminal emulation program for LXE devices with a Windows operating System, When RFTerm is installed, this icon is displayed on the desktop.

Desktop Icon	Function
	A shortcut to the Remote Desktop Configuration utility.
	Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help or run programs.

Taskbar Icons

The number and type of icons displayed in the taskbar are based on the device type, installed options and configuration of the LXE device.

My Device Folders

Folder	Description	Preserved upon Reboot?
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Program Files	Applications	No
System	Internal SD Flash Card (CAB file storage)	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	No

Start Menu Program Options

The following options represent the factory default program installation. Your system may be different based on the software and hardware options purchased.

Start | Programs

Communication		Stores Network communication options
	ActiveSync	Transfer files between a MX9 and a desktop computer
	Connect	Run this command after setting up a connection
	Start FTP Server	Begin connection to FTP server
	Stop FTP Server	End connection to FTP server
Summit		Set Summit radio / network parameters
Command Prompt		The command line interface in a separate window
Inbox		Microsoft Outlook mail inbox
Internet Explorer		Access web pages on the world wide Internet
RFTerm		Option. Terminal emulation application.
Media Player		Digital media player for movie and audio files.
Microsoft WordPad		Opens an ASCII notepad
Remote Desktop Connection		Log on to a Windows Terminal Server
Transcriber		Enter data using the stylus on the touchscreen
Windows Explorer		File management program

Note: The Microsoft File Viewers cannot display files that have been password protected.

- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- The wireless client connects automatically during each reboot.
- Bluetooth re-connects to nearby paired devices automatically at the conclusion of each reboot.

Communication

Start | Programs | Communication

ActiveSync Introduction

ActiveSync is pre-loaded on all LXE mobile devices.

Using Microsoft ActiveSync you can copy files from your MX9 to your desktop computer , and vice versa.

Once an ActiveSync relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, the infrared port, or USB on the MX9.

Connect and LXEConnect

Upon cabling your MX9 to the desktop/laptop, ActiveSync on the desktop/laptop opens. Contact your LXE representative for assistance if the Connect or LXEConnect installation does not open on yourMX9.

Start FTP Server / Stop FTP Server

These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

Summit

Start | Settings | Control Panel | Summit

Use this option to setup radio client profiles.

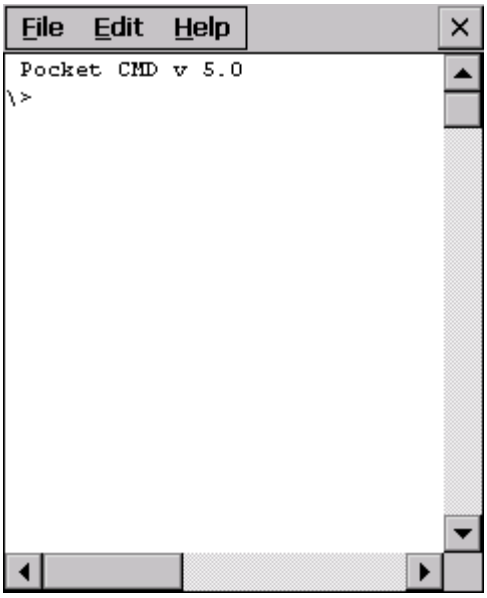
The Summit Control Panel can also be accessed by doubletapping the Summit icon in the taskbar or on the desktop.

Certs

The Certs option displays a readme file containing details on how the Summit Configuration Utility (SCU) handles certificates for WPA authentication.

Command Prompt

Start | Programs | Command Prompt



Type help at the command prompt for a list of available commands.

Exit the Command Prompt by typing **exit** at the command prompt or select **File | Close.**

Internet Explorer

Start | Programs | Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the "?" button to access Internet Explorer Help.

Media Player

Start | Programs | Media Player

There are few changes in the Windows CE version of Media Player as it relates to the general desktop Windows PC Microsoft Media Player options.

Click the "?" button to access Media Player Help.

Microsoft Wordpad

Start | Programs | Microsoft WordPad

Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft WordPad.

By default WordPad files are saved as .PWD files. Documents can be saved in other formats e.g. .RTF or .DOC.

Tap the ? button to access WordPad Help.

Remote Desktop Connection

Start | Programs | Remote Desktop Connection

There are few changes in the Windows CE version of Remote Desktop Connection as it relates to the general desktop Windows PC Microsoft Remote Desktop Connection options.

Select a computer from the drop down list or enter a host name and tap the Connect button.

Tap the Options >> button to access the General, Display, Local Resources, Programs and Experience tabs. Tap the “?” button to access Remote Desktop Connection Help.

Transcriber

Start | Programs | Transcriber

Select Transcriber on the Start | Programs menu. To make changes to the Transcriber application, enable or disable the current Transcriber session, etc., tap the “hand with a pen” icon in the toolbar. Tap the “?” button or the Help button to access Transcriber Help.

Windows Explorer

Start | Programs | Windows Explorer

There are a few changes in the Windows CE version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Tap the “?” button to access Windows Explorer Help.

Taskbar

Start | Settings | Taskbar and Start Menu

There are a few changes in the Windows CE version of Taskbar as it relates to the general desktop PC Windows Taskbar options. When the taskbar is auto hidden, press the Ctrl key then the Esc key to make the Start button appear.

General Tab

Factory Default Settings	
Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled

Taskbar Properties, General Tab

Advanced Tab

Taskbar Properties, Advanced Tab

Expand Control Panel

Tap the checkbox to have the Control Panel folders appear in drop down menu format from the Settings | Control Panel menu option.

Clear Contents of Document Folder

Tap the Clear button to remove the contents of the Document folder.

Taskbar Icons

As MX9 devices and applications open and change state, icons are placed in the Taskbar. In most cases, tapping the icon in the Taskbar opens the related application.

Refer to **Start | Help** for an explanation of standard Windows CE taskbar icons.

Following are a few of the MX9 and LXE unique taskbar icons that may appear in the Taskbar. These icons are in addition to the Windows CE taskbar icons.

Icon	Description
	Wireless Zero Config Inactive / Connected / Not Connected. Clicking on the icon opens the Wireless Zero Config utility.
	Bluetooth connected / disconnected. Clicking the icon opens the Bluetooth control panel.
	ActiveSync Connection
	Cerdisp connected (displayed when LXEConnect is connected)
	Summit Client signal indicator no signal/ excellent signal. Clicking on the icon opens the Summit Client Utility.
85	Battery charge indicator. Percent of battery charge is indicated.

Icon	Description
	External power connected
	Current time. Clicking the time display opens the Date/Time control panel.
	Click this icon to return to the Desktop.
	AppLock switchpad.
	Input method, keyboard / input panel / transcriber
	CapsLock active
	No modifier key is in focus
	Orange modifier key active
	Blue modifier key active
	Shift modifier key active
	Multiple modifier keys active, Shift plus Blue

ActiveSync

Introduction

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the MX9.

Requirement : ActiveSync version 3.8 (or higher) must be resident on the host (desktop/laptop) computer. ActiveSync for the PC is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync on your desktop computer.

Using Microsoft ActiveSync version 3.8 or higher, you can synchronize information on your desktop computer with the MX9 and vice versa. Synchronization compares the data on your mobile device with your desktop computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.

By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your desktop computer and your device.

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your device to your desktop computer,
- set up a partnership so you can synchronize information between your device and your desktop computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard. For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The initial setup of ActiveSync must be made via a USB or serial connection. When there is a Connect icon on the desktop, this section can be bypassed.

Partnerships can only be created using direct serial or USB cable connection. After the partnerships are established, ActiveSync communication can be initiated using:

- USB
- Serial
- Wireless

Connect via USB

The default connection type is **USB Client**

To change the connection type or to verify it is set to USB, select

Start | Settings | Control Panel | PC Connection

Tap the Change button. From the popup list, choose

USB Client

This will set up the mobile device to use the USB port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

IMPORTANT – DO NOT PUT THE MOBILE DEVICE INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

Connect the correct cable to the PC (the host) and the mobile device (the client) as detailed below. USB will start automatically when the USB cable is connected, not requiring you to select "Connect" from the start menu.

Cable for USB ActiveSync Connection:

MX9051CABLE - MX9 USB Client Cable Assembly (ActiveSync connection)

- Connect the I/O connector to the I/O port on the bottom of the MX9
- The USB client type A plug on the MX9 cable connects to a USB port on a PC or laptop.
- It is not necessary to connect the power receptacle to the MX9 power adapter in order to use ActiveSync. Do not allow the device to enter Suspend while connected.

Connect via Serial

The connection type must be changed to **Serial 1 @ 57600**.

To change the connection type select

Start | Settings | Control Panel | PC Connection

Tap the Change button. From the popup list, choose

Serial 1 @ 57600

This will set up the mobile device to use the serial port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

Select Start | Settings | Scanner and ensure the integrated scanner is set to a port that is NOT the same as the ActiveSync port.

Connect the correct cable to the PC (the host) and the mobile device (the client). Select "Connect" from the Start Menu on the client (Start | Programs | Communications | Connect).

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Cable for Serial ActiveSync Connection

Serial ActiveSync

MX9055CABLE - MX9 Serial Cable Assembly (ActiveSync connection)

- Connect the I/O connector to the I/O port on the bottom of the MX9
- The serial port on the MX9 cable connects to a COM port on a PC or laptop.
- It is not necessary to connect the power receptacle to the MX9 power adapter in order to use ActiveSync. Do not allow the MX9 to enter Suspend while connected.

Connect via Wireless

Note: You must establish a partnership with a desktop computer prior to running ActiveSync on the mobile device. The initial partnership must be done using direct, serial or USB cable connection.

Once the relationship is established using the serial port, the ActiveSync link in the Start Menu gives a choice of connections, one of which is Network.

Select Start | Settings | Programs | Communication | ActiveSync. From the popup list, choose Network and then tap the Connect button.

Synchronizing from the Mobile Device

To synchronize using a wireless LAN card, you must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device.

To initiate synchronization from your device, tap Start | Programs | Communication | ActiveSync to begin the process.

Tap **Sync** to connect and synchronize. View synchronization status.

Tap **Tools** to synchronize or change synchronization settings. View connection status.

Tap **Stop** to stop synchronization.

Tap **Start | Help** for context-sensitive help.

Explore

From the ActiveSync Dialog on the Desktop PC, tap the Explore button, which allows you to explore the mobile device from the PC side, with some limitations. You can copy files to or from the mobile device by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the mobile device. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows image. This, however, includes most of the files in the \Windows folder).

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

Prerequisites

A partnership between the mobile device and ActiveSync has been established.

Serial Port Transfer

- A desktop or laptop PC with an available serial port and a mobile device with a serial port. The desktop or laptop PC must be running Windows NT or greater.
- Null modem cable with all control lines connected. LXE recommends using the null modem cable part number listed in Connect and Communicate.

USB Transfer

- A desktop or laptop PC with an available USB port and a mobile device with a USB port. The desktop or laptop PC must be running Windows 98 SR2 or greater.
- Use the LXE-specific USB cable as listed in Connect Via USB.

Connect

Connect the modem cable to the PC (the host) and the mobile device (the client). Select "Connect" from the Start Menu on the mobile device (Start | Programs | Communications | Connect).

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Note: USB synchronization will start automatically when the cable is connected, not requiring you to select "Connect" from the Start menu.

Disconnect

USB Connection

- Disconnect the cable from the mobile device.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

IMPORTANT – Do not put the mobile device into Suspend while connected via USB. The device will be unable to connect to the host PC when it resumes operation.

Serial Connection

- Disconnect the cable from the mobile device.
- Put the mobile device into Suspend.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Network Connection

- Put the mobile device into Suspend.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Troubleshooting ActiveSync

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

If the MX9 is connected to a PC by a cable, disconnect the cable from the MX9 and reconnect it again.

Check that the correct connection is selected (Serial or USB “Client” if this is the initial ActiveSync installation).

See Also: “Cold Boot and Loss of Host Reconnection”.

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon (or REPLLOG.EXE in the Windows directory).

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

ActiveSync indicator on the host turns green and spins, but connection never occurs

Baud rate of connection is not supported or detected by host. Check that the correct connection is selected (Serial or USB “Client” if this is the initial ActiveSync installation).

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

The host doesn’t know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Testing connection with a terminal emulator program, or a serial port monitor

You can use HyperTerminal or some other terminal emulator program to do a rough test of ActiveSync. Set the terminal emulator to 8 bits, no parity, 1 stop bits, and the same baud rate as the connection on the CE device. After double-tapping REPLLOG.EXE on the CE device, the word “CLIENT” appears on the display in ASCII format. When using a serial port monitor, you see the host echo “CLIENT”, followed by “SERVER”. After this point, the data stream becomes straight (binary) PPP.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

When the mobile device is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (Control Panel | System | Device Name)

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy that partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

MX9 without Touchscreen

For a MX9, the touchscreen can be disabled. It may be easier to configure the MX9 using ActiveSync and LXEConnect rather than using the MX9 keyboard only.

Configuring the MX9 with LXEConnect

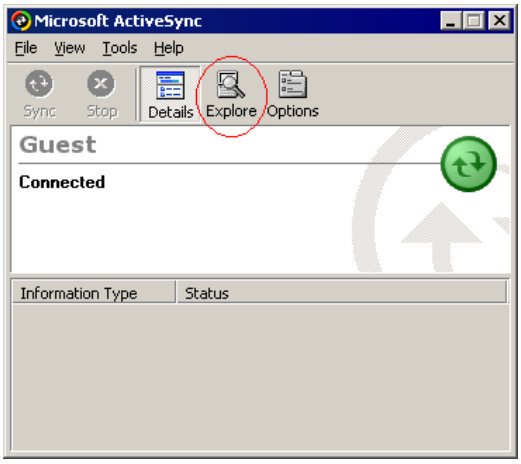
LXEConnect allows a user to view the MX9screen remotely from a PC using an ActiveSync connection:

Requirements: ActiveSync version 3.8 (or higher) must be resident on the host (desktop/laptop) computer. Please see the following section ActiveSync for more details on ActiveSync.

ActiveSync is already installed on the MX9. The MX9 is preconfigured to establish a USB ActiveSync connection to a PC when the proper cable is attached to the MX9 and the PC. If The MX9 uses a serial port for ActiveSync, it is necessary to configure the MX9 to use the serial port. Complete details on the proper cables and port configuration are included in the ActiveSync section.

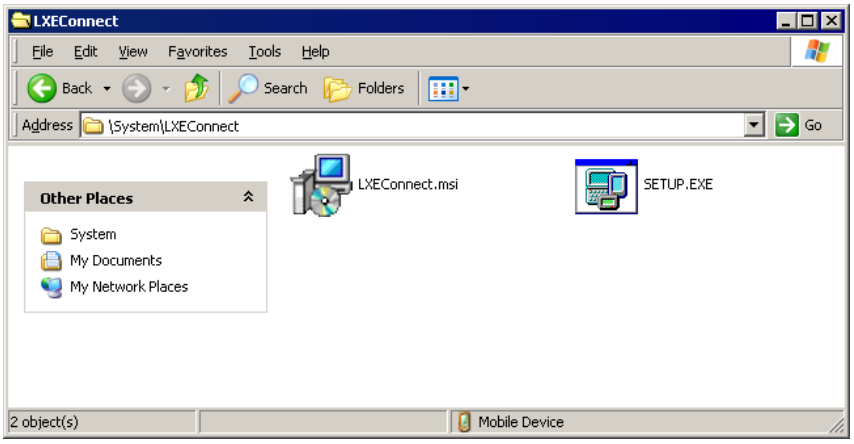
Install LXEConnect

1. Install Microsoft ActiveSync version 3.8 or higher on a PC with a USB port. For details, please see ActiveSync.
2. Power up the MX9.
3. Connect the MX9 to the PC using the proper connection cable. Once connected, the ActiveSync dialog box appears. If using the USB connection, the ActiveSync connection is automatically established. If using a serial connection, it is necessary to initiate the connection from the MX9.
4. Select “No” for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use LXEConnect. However, if a partnership is desired for other reasons, one may be established now. More details on partnerships are included in ActiveSync later in this chapter.
5. When the ActiveSync screen appears, select Explore.



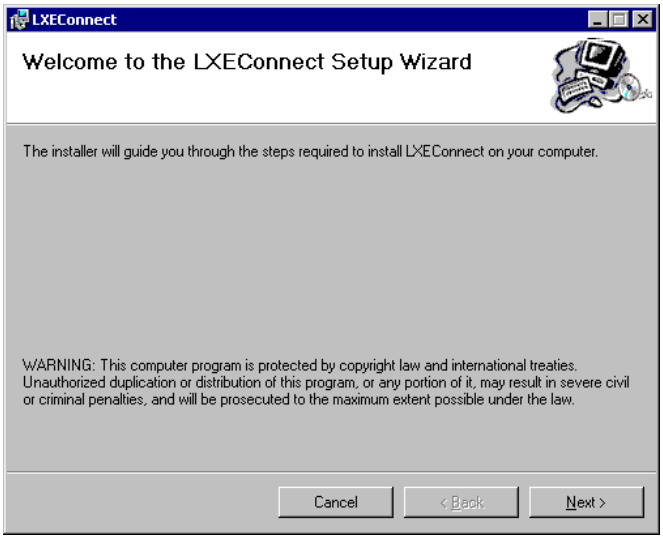
ActiveSync Explore

6. An explorer window is displayed for the MX9. Browse to the \System\LXEConnect folder. Contact your LXE representative for the necessary files if this folder is not present.



LXEConnect Installation Files

7. Select and copy the LXEConnect.msi and Setup.exe files from the MX9 to the user PC. Note the location chosen for files
8. Close the ActiveSync explorer dialog box. Do not disconnect the MX9 ActiveSync connection.
9. Execute the setup.exe file that was copied to the user PC. This setup program installs the LXEConnect utility.

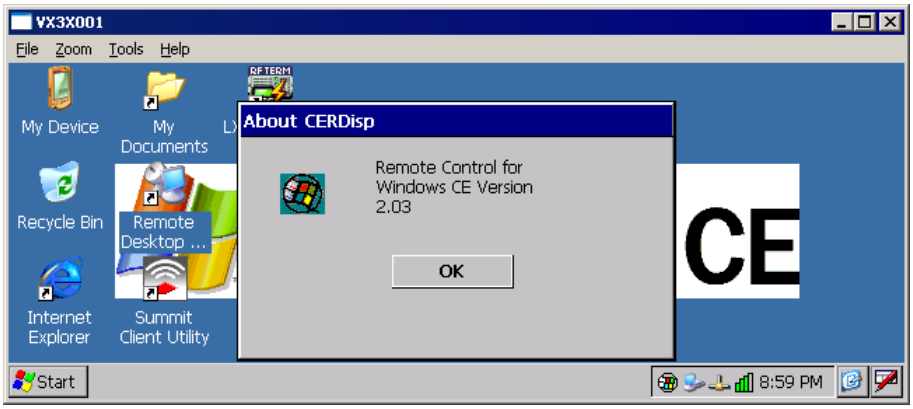

LXEConnect
Welcome to the LXEConnect Setup Wizard
The installer will guide you through the steps required to install LXEConnect on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

LXEConnect Setup

10. Follow the on screen installation prompts. The default installation directory is C:\Program Files\LXE\LXEConnect.
11. When the installation is complete, create a desktop shortcut to the following file: C:\Program Files\LXE\L-XEConnect\LXEConnect.exe. If a different directory was selected during installation, please substitute the appropriate directory.
12. LXEConnect is now installed and ready to use.

Using LXEConnect

1. If an ActiveSync connection is has not been established, connect the MX9 to the PC. Details on ActiveSync are included in the following section.
2. Double-click the LXEConnect icon that was created on the desktop.
3. LXEConnect launches.



LXEConnect Notice

4. Click the OK button to dismiss the About CERDisp dialog box. The dialog box automatically times out and disappears after approximately 30 seconds.

LXEConnect Desktop

5. The MX9 can now be configured from the LXEConnect window. Input from the PC's mouse and keyboard are recognized as if they were attached to the MX9.
6. When the remote session is completed, terminate the LXEConnect program by selecting File | Exit or clicking on the X in the upper right hand corner to close the application then disconnect the ActiveSync cable.

Note: After using LXEConnect, the MX9 cannot go into Suspend mode until after a warmboot. If using Power Management on a MX9, always warmboot the MX9 when finished using LXEConnect.

Control Panel

Start | Settings | Control Panel or My Device | Control Panel link

Note: Change the font displayed on the touchscreen by choosing Start | Settings | Control Panel | Keyboard and then the Key map drop down list.

Tap the ? button for Help when changing MX9 Control Panel options.

Option	Function
About	Software, hardware, versions and network IP. No user intervention allowed. Integrated scanner type is identified.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	LXE AppLock Administration utility.
Battery	View voltage and status of the main and backup batteries.
Bluetooth	Set the parameters for Bluetooth device connections.
Certificates	Manage digital certificates used for secure communication.
Data Collection (Wedge)	Wedge utility for data collected from barcode scans. Set data collection device, notifications, data stripping, prefix/suffix, and vibration (if installed) options. Assign baud rate, parity, stop bits and data bits for COM1 port. Assign collected data manipulation parameters.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings.
Dialing	Connection setup for modem attached to COM port or Compact Flash slot.
Display	Set background graphic and scheme. Set touchscreen and keypad backlight properties and timers.
Input Panel	Select the current key / data input method. Select custom key maps.
Internet Options	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate.
KeyMap	Configure KeyMap keys, RunCmd and LaunchApp.
Mixer	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touchscreen.
Network and Dial Up Options	Set network driver properties and network access properties.
Network Capture	Monitor and capture network activity.
Options	Set various device specific configuration options.
Owner	Set the mobile device owner details (name, phone, etc). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.
Password	Set OS access password properties for signon and/or screen saver.
PC Connection	Control the connection between the mobile device and a local desktop or laptop

Option	Function
	computer.
Peripherals	Enable or disable touch screen heater and scanner window heater, if installed. Set the flashlight off timer if the flashlight is installed. Use the GPS panel to toggle the GPS receiver on and off.
Power	Set Power scheme properties. Review device status and properties.
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs	Select to remove specific **user installed** programs in their entirety.
Registry	Load User Defaults, Save User Defaults, Load Factory Defaults, and Warmboot.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Terminal Server Client Licenses	Select a server client license from a drop down list.
Volume and Sounds	Enable / disable volume and sounds. Set volume parameters and assign sound WAV files to events.
WiFi	Set the parameters for a Summit client.
WWAN	Set parameters for the Wireless Wide Area Network client, if installed.

About

Start | Settings | Control Panel | About

The data cannot be edited by the MX9 user on these panels.

Tab	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language. Language indicates any pre-installed Asian fonts.
Hardware	CPU Type, Codec Type, Scanner type, Display, Flash memory, and DRAM memory
Versions	Revision level of LXE software modules and .NET Compact Framework Version. LXE Utilities, LXE Drivers, LXE Image, LXE API, and Internet Explorer.
Network IP	Current network connection IP and MAC address. Only the first 2 network ports are shown (usually radio and ActiveSync).

Version window information is retrieved from the registry.

Version Tab and the Registry

Modify the Registry using the Registry Editor. LXE recommends caution when editing the Registry and also recommends making a backup copy of the registry before changes are made.

The registry settings for the Version tab are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

To add a user application to the Version panel, create a new string value under the HKLM\Software\LXE\Version key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window .

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Language and Fonts

The Software tab displays any fonts built into the OS image. The fonts built into the OS image are noted in the Language section of this tab:

- English only – No additional fonts are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The above listed Asian fonts are ordered separately and built-in to the OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the (English only) default (extended) fonts.

When an Asian font is copied into the fonts folder on the /System folder; the font works for Asian web pages, the font works with RFTerm, the font does not work for Asian options in Regional Settings control panel, the font does not work for naming desktop icons with Asian names, the font does not work for third-party CE applications, the font does not work for some third-party MFC applications.

Identifying Software Versions

The Versions tab displays the versions of many of the software programs installed. Not all installed software installed on the mobile device is included in this list and the list varies depending on the applications loaded on the MX9. The LXE Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

MAC Address

The Network IP tab displays the MAC address of the network card.

Accessibility

Start | Settings | Control Panel | Accessibility

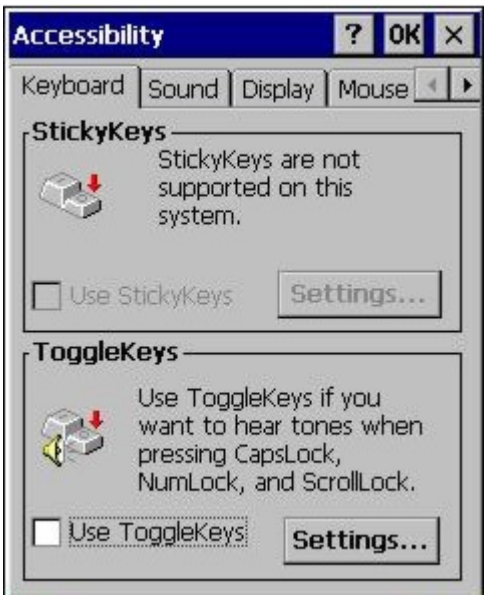
Customize the way the MX9 keyboard, sound, display, mouse, automatic reset and notification sounds function. There are a few changes from general Windows desktop Accessibility options.

Note: LXE disables the keypad StickyKeys and StickyKeys Settings on the Keyboard panel as this setting, when enabled, interferes with LXE's assigned sticky key implementation.

The following exceptions are due to a limitation in the Microsoft Windows CE operating system:

- If the ToggleKeys option is selected, please note that the ScrollLock key does not produce a sound as the CapsLock and NumLock keys do.
- If the SoundSentry option is selected, please note that ScrollLock does not produce a visual warning as the CapsLock and NumLock keys do.

Tab	Contents
Keyboard	Sticky Keys - Disabled. ToggleKeys - Disabled by default. Tap the *Use ToggleKeys* checkbox to enable this option. Tap the Settings button to view or change parameters.
Sound	SoundSentry is disabled by default. Tap the *Use SoundSentry* checkbox to enable this option. Tap the Settings button to view or change parameters.
Display	High Contrast is disabled by default. Tap the *Use High Contrast* checkbox to enable this option. Tap the Settings button to view or change parameters.
Mouse	MouseKeys is disabled by default. Tap the *Use MouseKeys* checkbox to enable this option. Tap the Settings button to view or change parameters.
General	Automatic reset is disabled by default. Tap the *Turn off accessibility features* checkbox to enable this option and use the drop down option to assign a timer. Notification is enabled by default. Sounds are emitted when turning a feature on or off.



Administration - for AppLock

Introduction

LXE's AppLock is designed to be run on LXE certified Windows CE based devices only. LXE loads the AppLock program as part of the LXE customer installation process.

MX9 AppLock is setup by the Administrator by tapping Start | Settings | Control Panel | Administration.

Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

The assumption, in this section, is that the first user to power up a new mobile device is the system administrator.

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other MX9 Control Panels.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

AppLock is updated periodically as new options become available. Contact your LXE representative for assistance, downloads and update availability.

Factory Default Settings - AppLock

Application Panel	
Filename	Blank
Title	Blank
Arguments	Blank
Order	1
Internet	Disabled
Global Key	Ctl+Spc / Ctrl+Spc
Global Delay	10 sec
Input Panel	Disabled
Launch Button Panel	
Auto at Boot	Enabled
Auto at Boot Retries	0
Auto at Boot Delay	10 sec
Auto Re-launch	Enabled
Auto Re-launch Retries	0
Auto Re-launch Delay	0 sec
Manual Launch	Disabled
Allow Close	Disabled
Security Panel	
Hotkey (Activation key) 62 key	Shft+Ctl+A
Hotkey (Activation key) 38 key	Shift+Ctrl+Alpha+2
Password	Blank
Status Panel	
Filename	\System\applock.txt
View Level	None
Log Level	None

Setup a New Device

LXE devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the MX9 is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies the applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

1. Connect an external power source to the device and press the Power button.
2. Adjust screen display, audio volume and other parameters if desired. Install accessories.
3. Tap Start | Settings | Control Panel | Administration icon.
4. Assign applications on the Application tab screen.
5. Assign a password on the Security tab screen.
6. Select a view level on the Status tab screen, if desired.
7. Tap OK
8. Press the hotkey sequence to launch AppLock and lock the configured application(s)
9. The device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device are:

Administrator Hotkey	Shift+Ctrl+A
Password	None
Application path and name	None
Application command line	None

End User Mode

End-user mode locks the end-user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user clicks on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g. missing DLLs).
- Corrupted registry settings.

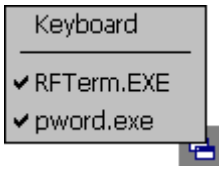
To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

Forgotten password?

See: Troubleshooting

End-User Switching Technique

Note: The touch screen must be enabled.



Switchpad Menu and Switchpad

A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the MX9 default input method (Input Panel, Transcriber, or custom input method) is activated.

The check to the left of the application name indicates that the application is active.

If the application is listed but does not have a checkmark to the left of the application name, this means the application is configured in AppLock and can be manually launched by clicking on the application name in the list.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the lower right corner of the display. The Switchpad is always visible on top of the application in focus. However, if only one application is configured in AppLock and the Input Panel is disabled the Switchpad is not visible.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.

See Also: Application Panel | Launch | Manual (Launch) and Allow Close

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the Activation key. The Activation key is assigned by the Administrator using the Global Key parameter. When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See Also: Application Panel | Global Key

Hotkey (Activation hotkey)

If the mobile device uses LXE's Multi AppLock to allow the user to switch between applications, the default Activation key is **Ctrl+Spc**. The key sequence switches the focus between one application and another. Data entry affects the application running in the foreground only. Note that the system administrator may have assigned a different key sequence to use when switching applications.

Application Configuration

Settings | Control Panel | Administration icon

The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

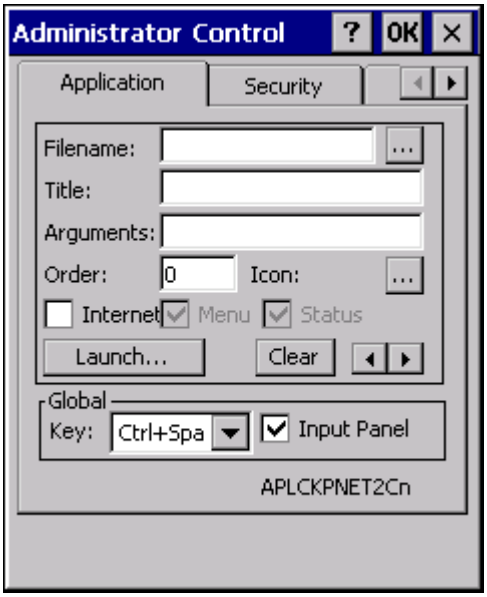
The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Important: Before setting up multiple instances of the same application, make sure the targeted software application will allow two instances to run at the same time.

Application Panel

Note: Users of Single-Application AppLock have a Control tab instead of an Application tab. Some of the options in this section do not apply to the Control tab.



Application Panel

Note: If your Application Panel does not look like the figure shown above, you may have the Single Application version.

Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

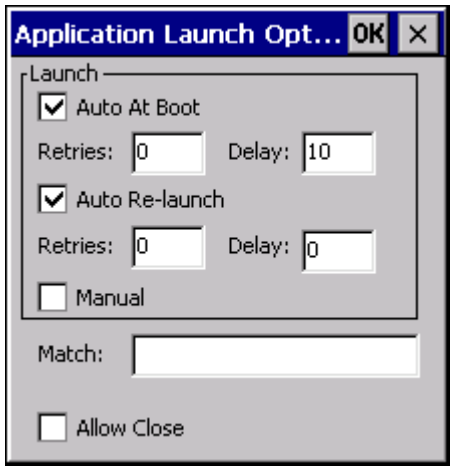
Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the Switchpad.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order and do not need to be sequential.
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE) When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End-user Internet Explorer (EUIE) for more details.
Launch Button	See following section titled Launch Button. *Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other LXE Control Panels.*
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global

Option	Explanation
	key is presented to the end-user as the Activation key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. *Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications. See Boot Options.*
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

Note: The Launch button may not be available in all versions of Multi-AppLock. Contact your LXE representative for assistance, downloads and AppLock update availability.

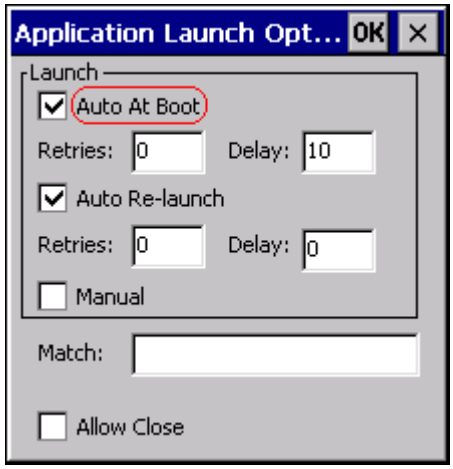
When clicked, displays the Launch options panel for the Filename selected on the Administration panel.



Application Launch Options

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto At Boot



Auto At Boot Settings

Default is Enabled.

Auto At Boot

When enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The

Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Retries

This is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Delay

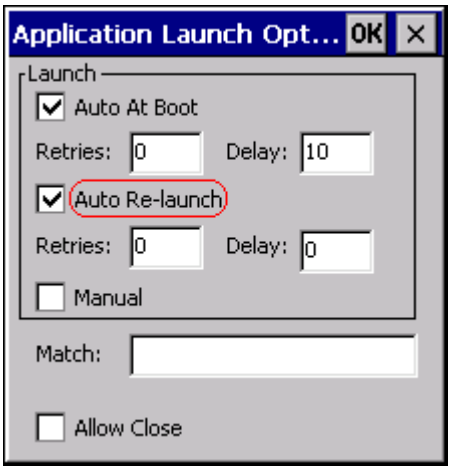
This timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch



Auto Re-launch Settings

Auto Re-Launch

Default is Enabled.

When enabled for a specific application. automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.

Retries

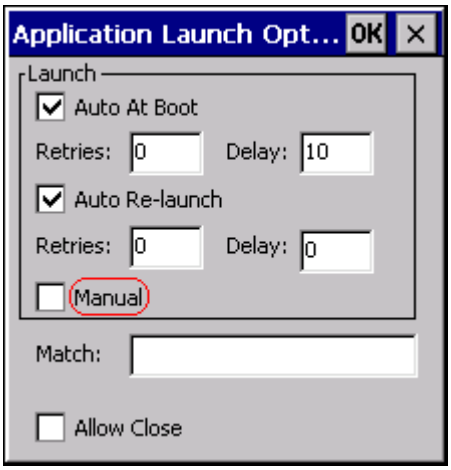
Default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Delay

Default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)



Manual Launch Checkbox

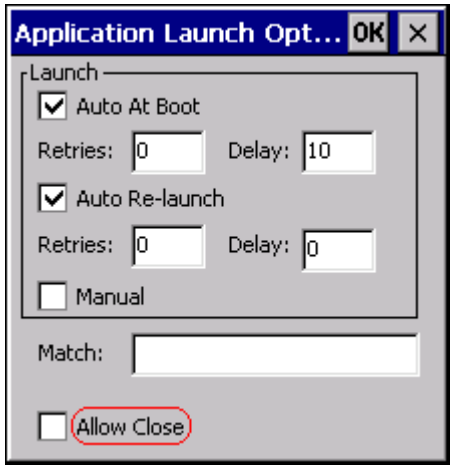
Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

Allow Close

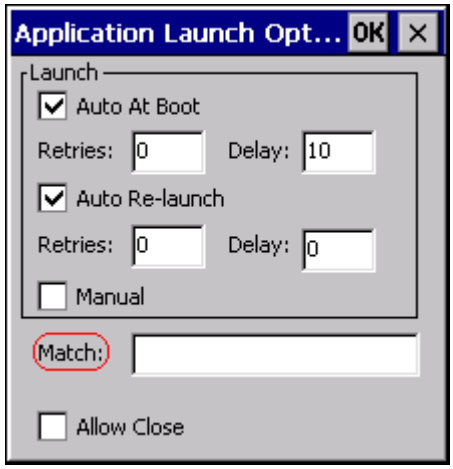


Allow Close Checkbox

Default is Disabled. When enabled, the associated application can be closed by the end-user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

Match



Match Textbox

Default is blank (match is not used).

AppLock works by associating display windows with the launched process ID. If an application uses different process IDs for windows it creates, the Match field must be used.

Use the Match field to specify up to 32 characters of the class name for the application.

For example, DOS applications using a standard DOS display box should specify **condev_appcls** in the Match textbox.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the Internet checkbox in the Application tab of the Administrator applet. The internet application should then be entered in the Application text box.

When the Internet checkbox is enabled, the Menu and Status check boxes are available.

Enabling the Menu checkbox displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel

Security Panel

Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with “Shift”, “Alt”, and “Ctrl” text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP are not guaranteed to work properly when switching operational modes.

For example, if the ‘Ctrl’ key is pressed followed by ‘A’, “Ctrl+A” is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Password

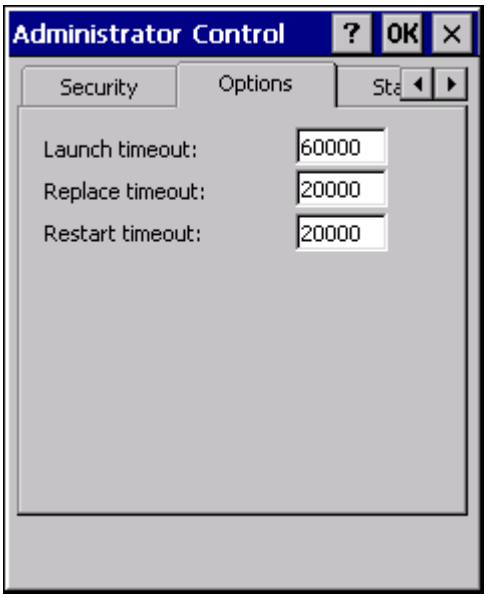
Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: Passwords and Troubleshooting

Options Panel

AppLock contains several types of delays and timeouts to accommodate different applications. Please note that the delays specified on the Launch panel are delays before AppLock attempts to start the specified application(s). The timesouts specified on this panel are delays after AppLock has attempted to launch the application.



Options Panel

Launch timeout

This timeout specifies the period of time for AppLock to wait for the application to initially launch after the application has been called. For example, if the application takes time to launch and then initialize before a display a window is created, use this delay to specify the delay period.

Replace timeout

This timeout specifies the period of time for AppLock to wait after an initial screen (like a password prompt screen) is replaced by another application window.

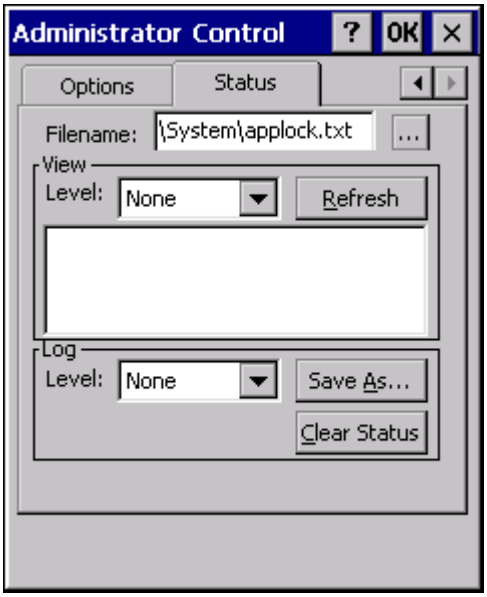
Restart timeout

This specifies the period of time for AppLock to wait for an application to restart. If the application fails to restart automatically, AppLock then proceeds according to the options selected when the application was configured on the Application and Launch panels.

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.



Status Panel

Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

Note: If your Status Panel does not look like the figure shown above, you may have the Single Application version which does not have as many options.

View

Error - Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.

Process - Processing status shows the flow control of AppLock components and is mainly intended for LXE Customer Service when helping users troubleshoot problems with their AppLock program.

Extended - Extended status provides more detailed information than that logged by Process Logging.

All - All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: Error Messages

Troubleshooting AppLock

The mobile device won't switch from Administration mode to end-user mode.

- If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.
- If two copies of the same application are configured, but the application only allows one copy to run at a time, for example Microsoft Pocket Word, the switch to end-user fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, the Administrator is not allowed to enter key combinations that are reserved by installed software applications. LXE has validated RFTerm key combinations ONLY.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

```
Selected hotkey is not allowed. Please reenter.
```

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

Can't locate the password that has been set by the administrator?

Contact your LXE representative for assistance.

Battery

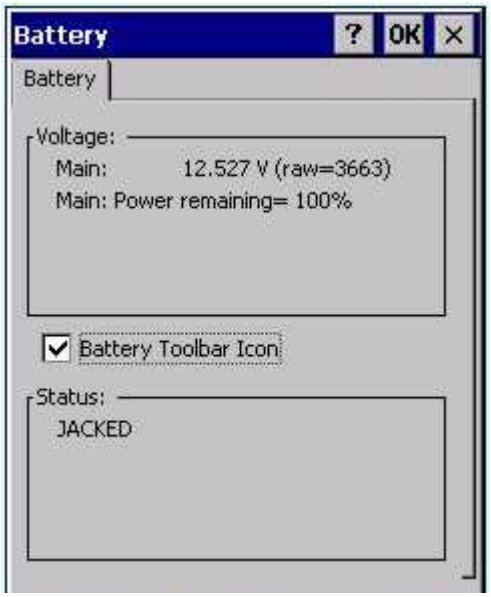
Start | Settings | Control Panel | Battery

This panel is used to view the status and percentage of power remaining in the MX9 main battery. The data cannot be edited by the user.

	The battery gas gauge icon resides in the system tray and shows four levels of charge – 100%, 75%, 50%, 25%. At a point below 50%, the system status LED will turn yellow and the gas gauge icon will turn yellow. At a point below 25%, the system status LED will turn red and the gas gauge icon will turn red indicating the battery is low.

Jacked is shown in the Status box when the Main battery is receiving external power.

The main battery is charged/recharged when the MX9 is docked in a powered cradle or directly cabled to an external power source.



The backup battery draws power from the Main battery to maintain a charge. The backup battery voltage and percentage of power fluctuate continuously.

When there is no Main battery in the unit, the backup battery begins to discharge as it maintains RAM and other vital settings. After a Main battery is installed, the backup battery begins to draw power from the Main battery again.

Note: Frequent connection to an external power source, if feasible, is recommended to maintain backup battery charge status as the backup battery cannot be recharged by a dead or missing main battery.

Bluetooth

Start | Settings | Control Panel | Bluetooth

Discover and manage pairing with nearby Bluetooth devices.

Factory Default Settings	
Discovered Devices	None
Settings	
Turn Off Bluetooth	Disabled
Report when connection lost	Enabled
Report when reconnected	Disabled
Report failure to reconnect	Enabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Disabled
Continuous search	Disabled

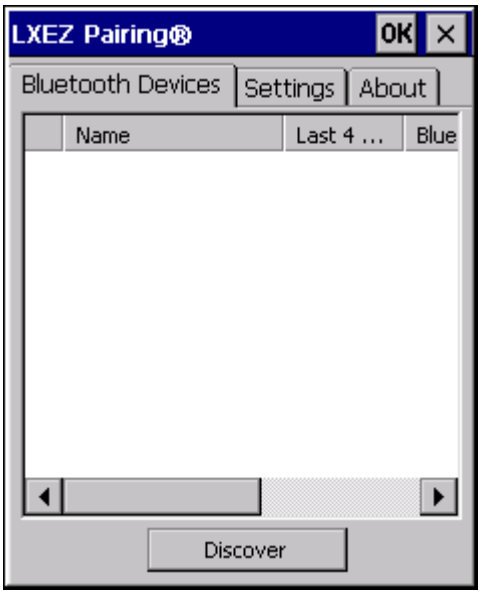
Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, pair, connect and disconnect. There may be audible or visual signals as paired devices re-connect with the MX9.

- The default Bluetooth setting is On.
- The MX9 cannot be discovered by other Bluetooth devices when the **Computer is discoverable** option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- The MX9 can pair with one Bluetooth scanner and one Bluetooth printer.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the MX9.
- The target Bluetooth device should be as close as possible (line of sight) to the MX9 during the pairing process.

Assumption:The System Administrator has Discovered and Paired targeted Bluetooth devices for the MX9. The MX9 operating system has been upgraded to the revision level required for Bluetooth client operation.

Bluetooth Devices

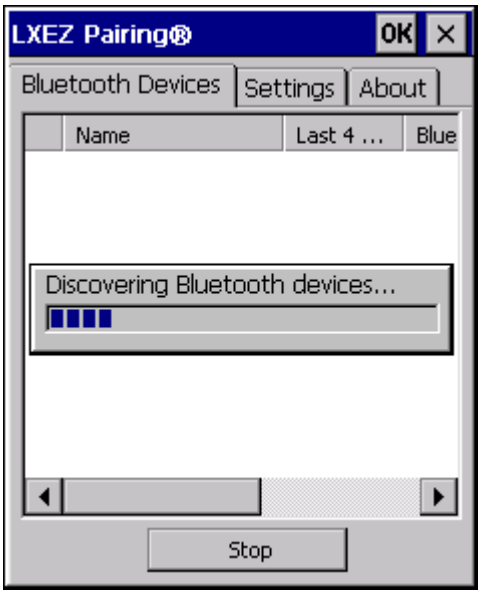
The Bluetooth Devices tab displays any device previously discovered and paired with the MX9.



Bluetooth Devices Panel

Discover

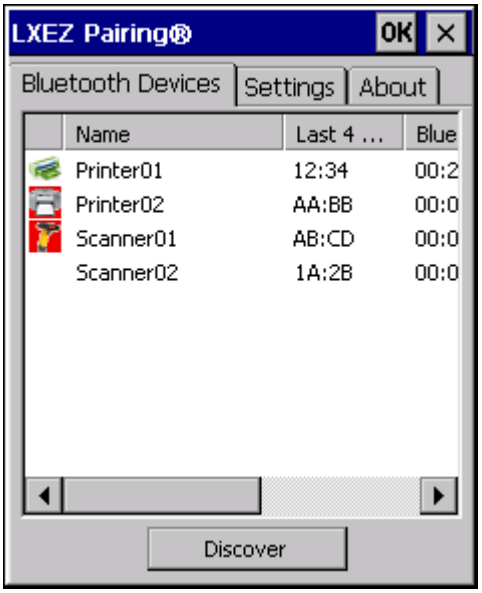
Tap the Discover button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier of each device discovered.



Discover Bluetooth Devices

Tap Stop at any time to end the Discover and Query for Unique Identifier functions.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the MX9 Bluetooth scanning range, the Bluetooth connection between the paired device and the MX9 is lost. There may be audible or visual signals as paired devices disconnect from the MX9.



Bluetooth Device List

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as printers or scanners. The Bluetooth panel assigns an icon to the device name.

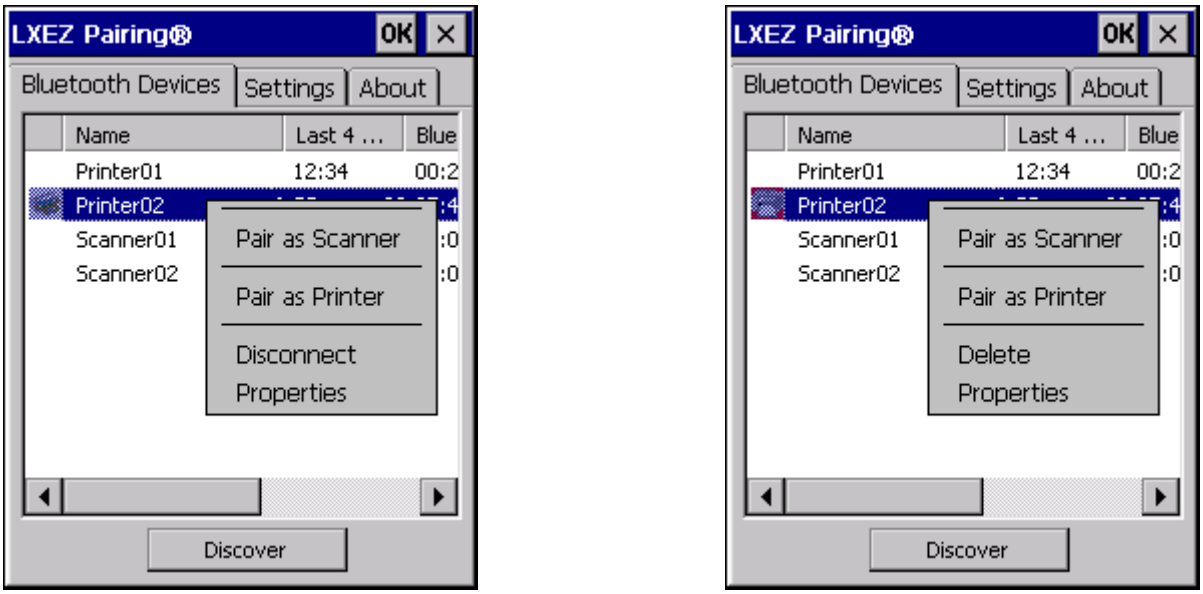
An icon with a red background indicates the device's Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the MX9 and the device's Bluetooth connection is active.

Double-tap a device in the list to open the device properties menu. The target device does not need to be active.

Bluetooth Device Menu

Doubleclick on a listed device to bring up the Bluetooth device menu.



Bluetooth Device Right Click Menu

Tap **Pair as Scanner** to set up the MX9 to receive data from the scanner.

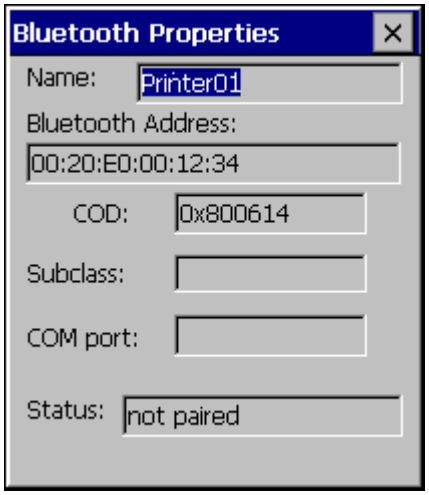
Tap **Pair as Printer** to set up the MX9 to send data to the printer.

Tap **Disconnect** (not shown) to stop the connection between the MX9 and a paired Bluetooth device.

Tap **Delete** to remove an unpaired device from the Bluetooth device list. The device name and identifier is removed from the MX9 Bluetooth Devices panel after the user taps OK.

Tap **Properties** for more information on the Bluetooth device.

Bluetooth Device Properties

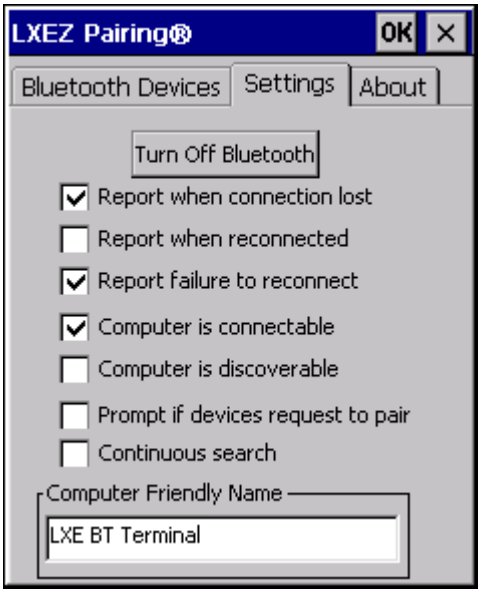


Bluetooth Device Properties Menu

Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.

Settings



Bluetooth Device Settings Panel

Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

Turn Off Bluetooth Button

Tap the button to toggle Bluetooth hardware On or Off.

Default

The default value is Bluetooth On.

Report when connection lost

A dialog box appears on the MX9 display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped.

Click the OK button or the X button to remove the dialog box from the screen.

Default

This option is enabled by default.

Report when reconnected

A dialog box appears on the MX9 display notifying the user a connection between one (or all) of the previously-paired Bluetooth devices is complete. This option is disabled by default.

Click the OK button or the X button to remove the dialog box from the screen.

Default

This option is enabled by default.

Report failure to reconnect

If the reconnect timeout (30 minutes) expires, a dialog box appears on the MX9 display notifying the end-user the connection between one (or all) of the previously-paired Bluetooth devices has failed. This option is enabled by default.

Click the OK button to remove the dialog box from the screen.

Default

This option is enabled by default.

Computer is connectable

There is no dialog connected to this checkbox. Enable this checkbox when you want the MX9 to be able to pair with other Bluetooth devices.

Default

This option is enabled by default.

Computer is discoverable

There is no dialog connected to this checkbox. Enable this checkbox when you want the MX9 to be Discovered by other Bluetooth devices.

Default

This option is disabled by default.

Prompt if devices request to pair

A dialog box appears on the MX9 screen notifying the user a Bluetooth device requests to pair with the MX9. This option is disabled by default.

The requesting Bluetooth device does not need to have been Discovered by the MX9 before the pairing request is received.

Click the Accept button or the Decline button to remove the dialog box from the screen.

Note: In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.

Default

This option is disabled by default.

Continuous search

When this checkbox is enabled, the MX9 never stops searching for a Bluetooth device it has paired with once the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off).

When this checkbox is disabled, the MX9 stops searching after one half hour. The search can be restarted by putting the MX9 through a Suspend/Resume cycle or accessing the Bluetooth control panel.

This option is disabled by default.

Default

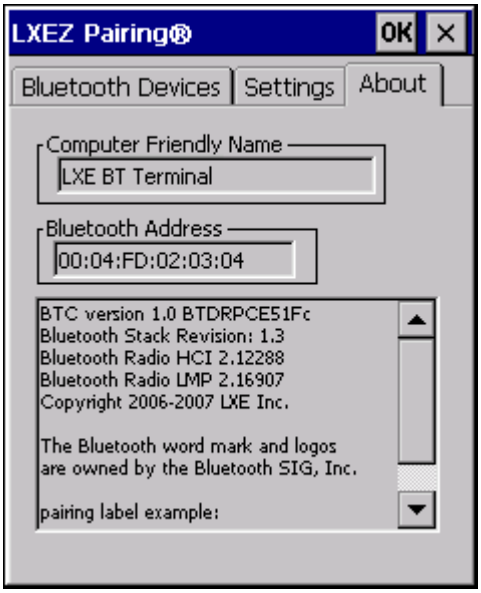
This option is disabled by default.

Computer friendly name

The name, or identifier, entered in this space by the System Administrator is used exclusively by Bluetooth operations.

*Note: The Device Name listed in **Start** | **Settings** | **Control Panel** | **System** | **Device Name** is not used during Bluetooth operation. Owner Identification name listed in **Start** | **Settings** | **Control Panel** | **Owner** | **Identification** is not used during Bluetooth operation.*

About



Bluetooth About Panel

This panel lists the assigned Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth MAC address, and software version levels. The data cannot be edited by the user.

Using Bluetooth

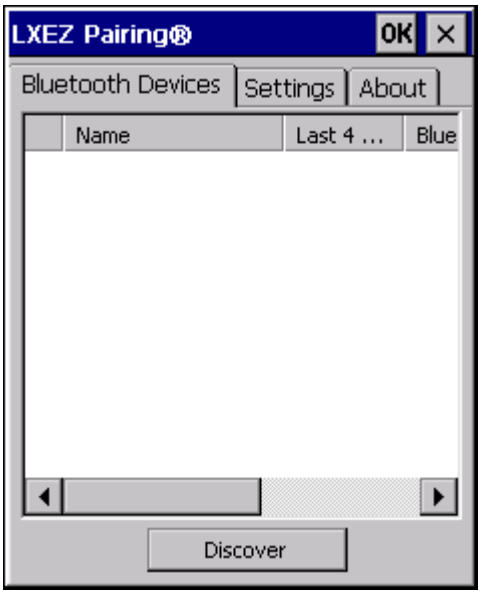
Start | Settings | Control Panel | Bluetooth or Bluetooth icon in taskbar or Bluetooth icon on desktop

The MX9 default Bluetooth setting is Enabled.

The LXE MX9 Bluetooth® module is designed to Discover and pair with nearby Bluetooth devices.

Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.

Prerequisite: The Bluetooth devices have been setup to allow them to be "Discovered" and "Connected/Paired". The System Administrator is familiar with the pairing function of the Bluetooth devices.



Bluetooth Devices Display – Before Discovering Devices

Initial Use

1. Select **Start | Settings | Control Panel | Bluetooth** or tap the Bluetooth icon in the taskbar or on the desktop.
2. Tap the Settings Tab.
3. Change the Computer Friendly Name at the bottom of the Settings display. The Bluetooth MX9 default name is determined by the factory installed software version. LXE strongly urges assigning every MX9 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the MX9 Bluetooth options on the Settings tab.
5. Tap the OK button to save your changes or the X button to discard any changes.

Subsequent Use

Note: Taskbar and Bluetooth device Icon states change as Bluetooth devices are discovered, pair, connect and disconnect. A taskbar Bluetooth icon with a red background indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.

1. Tap the Bluetooth icon in the taskbar or on the desktop to open the Bluetooth LXEZ Pairing application.
2. Tap the Bluetooth Devices tab.
3. Tap the Discover button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth Devices window.
5. Highlight a Bluetooth device in the Discovered window and double-tap to open the device properties menu.
6. Tap Pair as Scanner to set up the MX9 to receive scanner data.
7. Tap Pair as Printer to set up the MX9 to send data to the printer.
8. Tap Disconnect to stop pairing with the device. Once disconnected, tap Delete to remove the device name and data from the MX9 Bluetooth Devices list. The device is deleted after the OK button is clicked.
9. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the MX9 display.
10. Whenever the MX9 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the MX9. If the devices cannot connect to the MX9 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if Report Failure to Reconnect is disabled.

Bluetooth Indicators

The Bluetooth taskbar Icon state and Bluetooth LED state change as Bluetooth devices are discovered, pair, connect and disconnect.

There may be audible or visual signals as paired devices re-connect with the MX9.

Only LXE printers or scanners are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.

Taskbar Icon	Legend
	Bluetooth module is connected to one or more of the targeted Bluetooth device(s).
	MX9 is not connected to any Bluetooth device. MX9 is ready to connect with any Bluetooth device. MX9 is out of range of all paired Bluetooth device(s). Connection is inactive.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the MX9 Bluetooth scan range, the Bluetooth connection between the paired device and the MX9 is lost. There may be audible or visual signals as paired devices disconnect from the MX9.

Bluetooth LED	Legend
Blue, blinking slowly	Bluetooth is active but not connected to a device.
Blue, blinking medium	Bluetooth is paired and connected to a device.
Blue, blinking fast	Bluetooth is discovering other Bluetooth devices.
Off	Bluetooth hardware has been turned off or does not exist in theMX9.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the MX9 while AppLock is in control. .

Bluetooth Barcode Reader Setup

Please refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Contact your LXE representative for Bluetooth product assistance.

Introduction

LXE supports several different types of barcode readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the MX9 using Bluetooth functions.

Prerequisites

- The MX9 has the Bluetooth hardware and software installed. An operating system upgrade may be required. Contact your LXE representative for details.
- If the MX9 has a Bluetooth address identifier barcode label affixed, then Bluetooth hardware and software is installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The MX9 main battery is fully charged. Alternatively, the MX9 may be in a powered cradle or cabled to AC/DC power.
- ***Important****: The barcode numbering examples in this segment are not real and should not be created nor scanned with a Bluetooth scanner.*
- To open the LXEZ Pairing program, tap **Start | Settings | Control Panel | Bluetooth** or tap the Bluetooth icon on the desktop or tap the Bluetooth icon in the taskbar.

Sample Bluetooth Address Barcode Label

Locate the barcode label, similar to the one shown above, attached to the MX9. The label is the Bluetooth address identifier for the MX9.

The mobile Bluetooth scanner / imager requires this information before discovering, pairing, connecting or disconnecting can occur.

Important: The MX9 Bluetooth address identifier label should remain protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth barcode readers.

MX9 with Label

If the MX9 has a Bluetooth address barcode label attached, follow these steps:

1. Scan the Bluetooth address barcode label, attached to the MX9, with the LXE Bluetooth mobile scanner.
2. If this is the first time the Bluetooth scanner has scanned the MX9 Bluetooth label, the devices are paired. See section titled "Bluetooth Beep and LED Indications". If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pairing panel [Start | Settings | Control Panel | Bluetooth].
4. Tap Discover. Locate the Bluetooth scanner in the Discovery panel.
5. Double-tap the stylus on the Bluetooth scanner. The right-mouse-click menu appears.
6. Select Pair as Scanner to pair the MX9 with the Bluetooth mobile scanner.

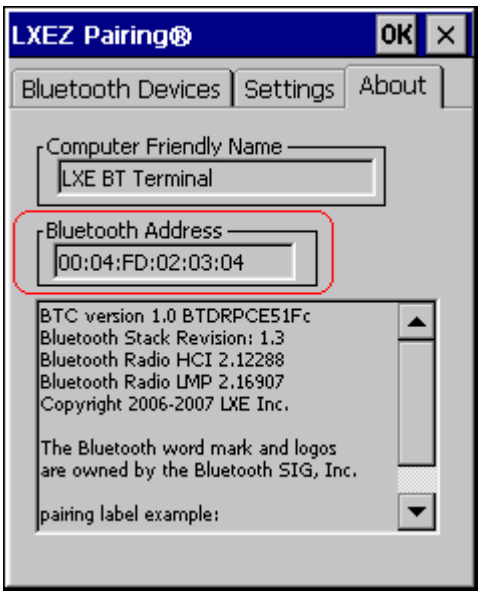
The devices are paired. The Bluetooth barcode reader responds with a series of beeps and an LED flashes. Refer to the following section titled "Bluetooth Beep and LED Indications".

Note: After scanning the MX9 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

MX9 without Label

If the MX9 Bluetooth address barcode label does not exist, follow these steps to create a unique Bluetooth address barcode for the MX9:

First, locate the MX9 Bluetooth address by tapping Start | Settings | Control Panel | Bluetooth | About tab.



About Tab and Bluetooth Address

Next, create a Bluetooth address barcode label for the MX9.

Note: Free barcode creation software is available for download on the World Wide Web. Search using the keywords "barcode create".

The format for the barcode label is as follows:

- Barcode type must be Code 128.
- FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). For example, LnkB0400fd002031.

Create and print the label.

Scan the MX9 Bluetooth address barcode label with the Bluetooth barcode reader.

The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes. Refer to the following section titled “Bluetooth Beep and LED Indications”.

Note: After scanning the MX9 Bluetooth label, if there is no beep and no LED flash from the Bluetooth device, the devices are currently paired.

Bluetooth Beep and LED Indications

Beep Type from Bluetooth Device	Behavior
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

LED on Bluetooth Device	Behavior
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact your LXE representative for assistance.

Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the end-user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of and then returned within range. Pairing supports SPP devices only.

Up to two Bluetooth devices can be connected to the MX9 at a time; LXE supports one Bluetooth scanner and one Bluetooth printer.

Note: Configuration elements are persistent and stored in the registry.

Setup the Bluetooth module to establish how the user is notified by easy pairing and auto-reconnect events.

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the MX9 while AppLock is in control.

Certificates

Start | Settings | Control Panel | Certificates

Manage digital certificates used for secure communication.

Note: Digital certificates are date sensitive. If the date on the MX9 is incorrect, wireless authentication will fail.

The Certificates stores lists the certificates trusted by the MX9 mobile device user.

These values may change based on the type of network security resident in the client, access point or the host system.

Tap the **Import** button to import a digital certificate file.

Tap the **View** button to view a highlighted digital certificate.

Tap the **Remove** button to remove highlighted certificate files.

Tap the ? button and follow the instructions in the Windows CE Help file when working with trusted authorities and digital certificates.

Data Collection Wedge

Start | Settings | Control Panel | Data Collection

Data Collection Wedge (or DCWedge) supports up to three concurrent data collection devices. For example, the internal scanner could be used to collect data at the same time that a Bluetooth scanner is paired and/or a serial device is connected to COM1.

This software component is the interface between data collection devices such as barcode scanners, or imagers, integrated into your MX9, barcode scanners externally connected to it's COM port or barcode scanners wirelessly connected via Bluetooth to your MX9. This software component collects the data from the varied sources and presents it to applications on your MX9 in a transparent manner.

Note: When a HID enabled USB scanner is connected to the MX9 the scanned data is transmitted to the active window as keystroke messages. The data bypasses the data collection wedge. Any data handling to be applied to the scanned data, for example strip leading or trailing characters, must be programmed into the scan engine via configuration barcodes or handled by the application accepting the data.

Use the options on the control panels to set MX9 data collection keyboard wedge parameters, enable or disable allowed symbologies, set the active scanner port, and assign scan key settings.

Assign baud rate, parity, stop bits and data bits for available COM ports.

Parameters on the Main tab and the COM tab(s) apply to this device only.

Barcode manipulation parameter settings on the Data Options tab are applied to the incoming data resulting from successful barcode scans received by the MX9 for processing. The successful barcode scan data may be sent by

- an integrated scanner in the endcap,
- a wireless Bluetooth Handheld Scanner,
- or a tethered scanner.

Since Internal is the default setting for Device 2, a Bluetooth scanner can be paired with DCWedge using LXEZ Pairing (on Device 1) without disabling the internal or integrated scanner.

Integrated scanner configuration can be changed using the Data Collection Control Panel or via the LXE Scanner API functions. While the changed configuration is being stored, the Scanner LED is solid amber. The scanner is not operational during the configuration update.

Note: The integrated scan engine begins scanning when the designated Scan key on the MX9 is activated.

When using any barcode reader to scan the Reset All (or equivalent) barcode (available in the Integrated Scanner Programming Guide) with the MX9's integrated scan engine, the next step is to open Data Collection on the MX9, click the OK button and then close it. This action will synchronize all scanner formats.

Barcode Readers

Your MX9 may be using any of the following barcode readers:

- Symbol SE955 Scanner
- Symbol SE1524 Scanner
- HHP 5300SF Imager

Tethered scanners (LXE 8500 series tethered to a serial port on the device or cradle) are configured by scanning the engine-specific barcodes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the barcode reader.

LXE wireless Bluetooth 8700 and 8800 series are configured by scanning the engine-specific barcodes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the barcode reader.

The LXE Bluetooth Ring Scanner (8650) module may be using a Symbol SE4400 Imager ring or a Symbol SE955 Scanner ring. The BTRS module is configured by scanning the barcodes in the *Bluetooth Ring Scanner Guide*.

Symbol scan engine specific barcodes are contained in the Integrated Scanner Programming Guide. They can be used to set or reset scan engine parameters by scanning a barcode, then saving the change. Symbol scan engines can be programmed using programming barcodes.

The HHP 5300 Imager engine is programmed by using the HHP Properties button (**Start | Settings | Control Panel | Data Collection Wedge**) on the Data Options tab and the Advanced button available on many of the individual Symbology Settings screens to configure the HHP Imager engine. There are no configuration barcodes for the HHP Imager.

Data Processing Overview

Barcode data processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Data Options control panels. The steps are presented below in the order they are performed on the scanned data.

1. Scanned data is tested for a **code ID** and length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the barcode data is processed based on the settings for All.
2. If the symbology is **disabled**, the scan is rejected.
3. Strip **leading** data bytes unconditionally.
4. Strip **trailing** data bytes unconditionally.
5. Parse for, and strip if found, **Data Options** strings.
6. Replace any **control characters** with string, as configured.
7. Add **prefix** string to output buffer.
8. If **Code ID** is ***not*** stripped, add saved **code ID** from above to output buffer.
9. Add processed **data string** from above to output buffer.
10. Add **suffix string** to output buffer.
11. Add a terminating **NUL** to the output buffer, in case the data is processed as a string.
12. If key output is enabled, start the process to output keys. If control characters are encountered:
    - If Translate All is set, key is translated to CTRL + char, and output.
    - If Translate All is not set, and key has a valid VK code, key is output.
    - Otherwise, key is ignored (not output).
13. If key output is disabled, a windows message is broadcast to notify listening applications that data is available.

The manipulated data is ready to be read by applications.

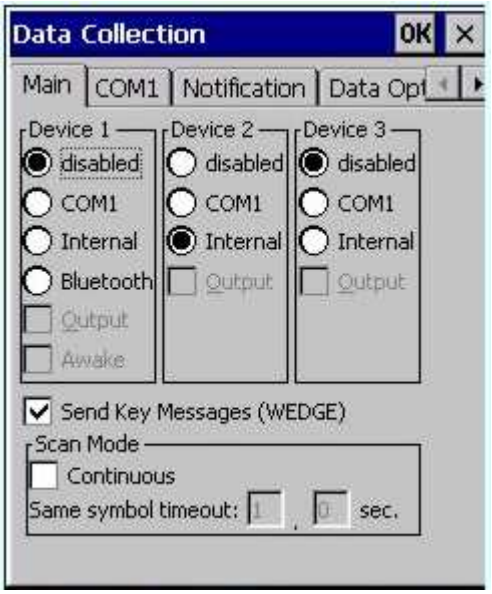
Factory Default Settings

Main Tab	
Device 1	Disabled
Device 2	Internal
Device 3	Disabled
Scan Mode - Continuous	Disabled
Same Symbol Timeout	Dimmed (1.0s)
Send Key Message (WEDGE)	Enabled
COM1 Tab (External serial port)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Power on Pin 9	Disabled
Notification Tab	
Enable Internal Scanner Sound	Enabled
Good Scan Vibration	Off
Bad Scan Vibration	Off
Data Options	
Enable Code ID	None
Symbology Settings	All
Control Character Translate All	Disabled
Custom IDs	Name blank
HHP Properties	Options Disabled: Centering DecodeMode LinearRange AimTimer LeaveLightsOn

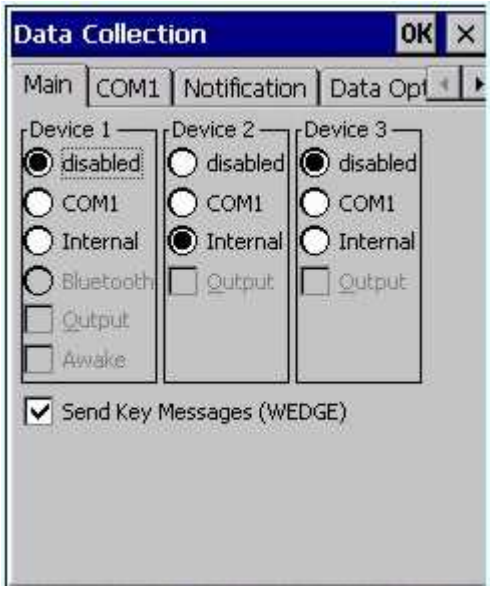
Main Tab

Start | Settings | Control Panel | Data Collection | Main tab

The parameters shown on these panels are only those that apply to the specific mobile device.



Device with Symbol Scanner



Device with HHP Imager

Note: The Scan Mode (Continuous Scan) section is only present if the MX9 has a Symbol integrated scanner.

Parameter	Function
Device 1,2,3	1 - Default is Disabled 2 - Default is Internal 3 - Default is Disabled The data collection **device** (laser scanner, laser imager, internal, external, or wireless).
Keep Awake	Default is Disabled.
Scan Mode	Default is Disabled. This box is only shown when the internal scanner is a Symbol scanner.
Send Key Messages (WEDGE)	Default: Enabled. When Send Key Messages (WEDGE) is checked any data collection scan is converted to keystrokes and sent to the active window. When this checkbox is not checked, the application will need to use the set of LXE Scanner APIs to retrieve the data from the scanner driver. Note that this latter method is significantly faster than using Wedge.

? OK X Tap the OK button to save changes and exit the control panel. Changes are saved across the Properties tabs.

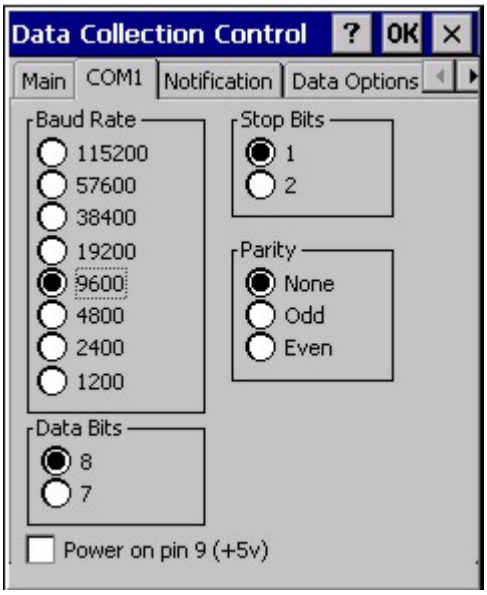
A message may be displayed that a warm boot is necessary otherwise changes are in effect immediately.

Tap the X button to ignore the current properties changes and exit the control panel.

Tap the ? button for help.

COM1 Tab

Start | Settings | Control Panel | Data Collection | COM1



This panel sets communication parameters for any device connected to the external port.

Adjust the settings and click the OK button to save the changes. Any changes take effect immediately.

This panel does not configure the connected device. Please refer to the documentation for the external connected or wireless device for information on configuring the device.

Note: COM default values are restored after a cold boot or operating system upgrade.COM1 supports 5V switchable power on Pin 9 for tethered scanners.

Integrated laser scanner default values are 9600 Baud, 8 data bits, 1 stop bit and No parity. If these values are changed, the default values are restored after a cold boot or reflashing.

Power on Pin 9

To configure the COM port to supply power to an external scanner tethered to the COM1 port, check the checkbox for Power on Pin 9 (+5V). The default is Off (disabled).

The external scanner is powered by the external device power source.

Wireless external scanners use their own power source.

Tap the OK button to save changes and exit the control panel. Changes are saved across the Properties tabs.

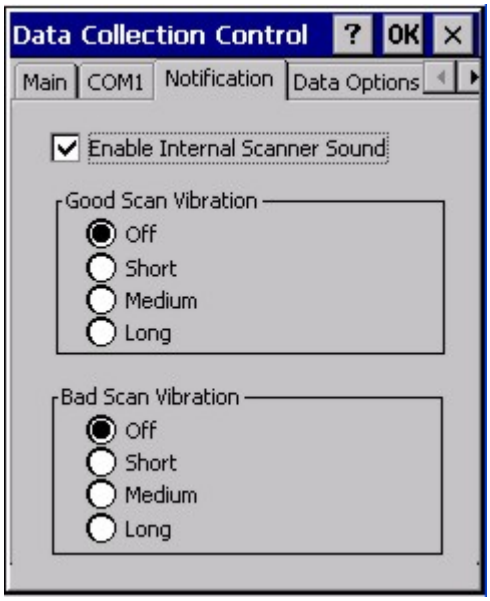
A message may be displayed that a warm boot is necessary otherwise changes are in effect immediately.

Tap the X button to ignore the current properties changes and exit the control panel.

Tap the ? button for help.

Notification Tab

Start | Settings | Control Panel | Data Collection | Notification tab



Internal Scanner Sound

This panel toggles internal scanner sounds on and off. Internal scanner sound, by default, is on (enabled).

Vibration

Vibration on the MX9 is activated when a scan is completed successfully or with a failure (scan key released before good scan, timeout, or rejected because of Data Options configuration). It is not activated when a trigger or scan key is pressed. The default setting for both Good Scan and Bad Scan vibration is Off.

Enable this parameter when a tactile response on a good scan or bad scan is desired. Scan sounds are accompanied by a tactile response when the internal scanner Sound parameter is enabled. Enable short, medium or long duration for each selection (good scan and bad scan).

When the MX9 does not have vibrate capability, any active vibration setting is ignored.

Tap the OK button to save changes and exit the control panel. Changes are saved across the Properties tabs.

A message may be displayed that a warm boot is necessary otherwise changes are in effect immediately.

Tap the X button to ignore the current properties changes and exit the control panel.

Tap the ? button for help.

Data Options Tab

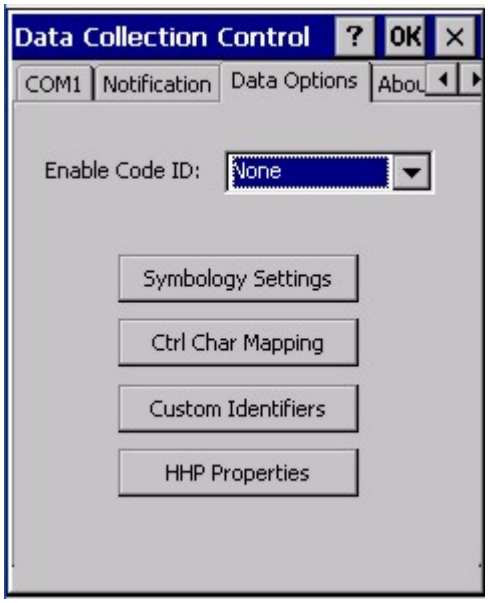
Start | Settings | Control Panel | Data Collection | Data Options tab

Barcode manipulation parameter settings on this tab are applied to the incoming data resulting from successful barcode scans sent to the MX9 for processing.

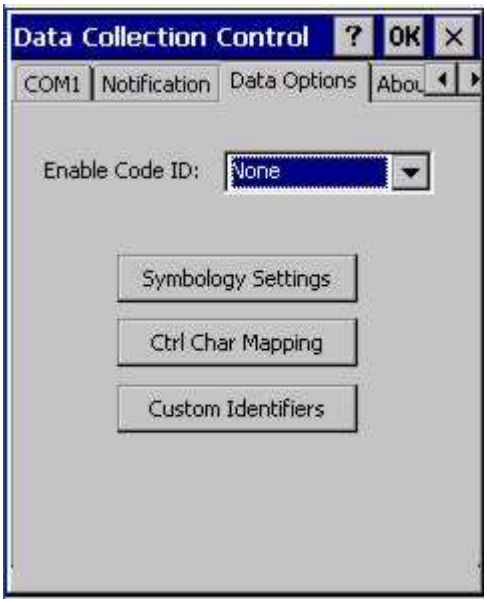
Note: The Data Options tab contains only those options available for one type of decoding engine.

The Data Options tab contains several options to control barcode processing. Options include:

- Defining custom Code IDs
- Disable processing of specified barcode symbologies
- Rejecting barcode data that is too short or too long
- Stripping characters including Code ID, leading or trailing characters and specified barcode data strings
- Replacing control characters
- Adding a prefix and a suffix.



MX9 with an HHP imager



MX9 with any other imager/scanner

Enable Code ID

This parameter programs the internal scanner to transmit the specified Code ID and/or determines the type of barcode identifier being processed. If the scanner being configured is not an integrated scanner, the scanner driver expects that the setting has been programmed into the scanner externally, and that the data will be coming in with the specified Code ID attached.

Transmission of the Code ID is enabled at the scanner for all barcode symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.

Choose an option in the Enable Code ID drop down box:

None	Disables transmission of a Code ID. The only entry in the Symbology combo box is **All**.
AIM ID	Transmits the AIM ID with each barcode. The combo box in the Symbology panel is populated with the known AIM ID symbologies for the scan engine in focus, plus any configured Custom code IDs.
Symbol ID	Transmits the Symbol ID with each barcode. The combo box in the Symbology panel is populated with the known Symbol ID symbologies for the scan engine in focus, plus any configured Custom code IDs.
HHP ID	The imager always transmits the HHP ID with each barcode, so the Code ID is used to identify the barcode being processed. The combo box in the Symbology control panel is populated with the known HHP ID symbologies for that platform, plus any configured Custom code IDs.
Custom ID	Does not change the scanner's Code ID transmission setting. The combo box in the Symbology control panel is populated with any configured Custom code IDs.

- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the barcode data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e. treated as a Code ID).
- UPC/EAN Codes only: The code id for supplemental barcodes is not stripped.
- When Enable Code ID is set to AIM, HHP or Symbol, Custom Code IDs appear at the end of the list of standard Code IDs.
- When Enable Code ID is set to Custom, Custom Code IDs replace the list of standard Code IDs.
- When Enable Code ID is set to Custom, AIM or Symbol Code IDs must be added to the end of the Custom Code ID. For example, if a Custom Code ID 'AAA' is created to be read in combination with an AIM ID for Code 39 ']A1', the Custom Code ID must be entered with the AIM ID code first then the Custom Code ID :]A1AAA. This note applies only to Symbol or EV-15 scanners because they are configured using configuration barcodes. Thus is AIM or Symbol Code IDs are enabled at the scanner, they must be included in the custom.
- When Enable Code ID is set to None, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- The external scanner operation cannot be controlled by the MX9 scanner driver; therefore, a 'good' beep may be sounded from the external scanner even if a barcode from an external scanner is rejected because of the configuration specified. The MX9 will still generate a 'bad' scan beep, to indicate the barcode has been rejected.

Buttons

Symbology Settings	Individually enable or disable a barcode from being scanned, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode before transmission.
Ctrl Char Mapping	Define the operations the LXE Wedge performs on control characters (values less than 0x20) embedded in barcodes.
Custom Identifiers	Defines an identifier that is at the beginning of barcode data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier just like standard Code IDs.
HHP Properties	HHP Properties allows HHP global (not symbology specific) parameters to be configured. This button is only visible when an HHP 5300 imager is installed in the MX9.

See "Barcode Processing Overview".

Tap the OK button to save changes and exit the control panel. Changes are saved across the Properties tabs.

A message may be displayed that a warm boot is necessary otherwise changes are in effect immediately.

Tap the X button to ignore the current properties changes and exit the control panel.

Tap the ? button for help.

Data Options - Symbology Settings

Start | Settings | Control Panel | Data Collection | Data Options | Symbology Settings button

The Symbology selected in the Symbology drop down list defines the symbology for which the data is being configured. The features available on the Symbology panel include the ability to

- individually enable or disable a barcode from scanning,
- set the minimum and maximum size barcode to accept,
- strip Code ID,
- strip data from the beginning or end of a barcode,
- or (based on configurable Barcode Data) add a prefix or suffix to a barcode.

The Code ID drop down box only filters the available symbologies in the Symbology drop down box by the selected Code ID. This Code ID box does not enable or disable the Code ID as that function is controlled by the Enable Code ID box on the Data Options tab.

The Symbology drop down box contains all symbologies supported based on the Code ID selected above. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the ok button is tapped. Settings are also saved when a new Symbology is selected from the Symbology drop down list.

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix / Suffix

*Note: When **Enable Code ID** is set to **None** on the Data Options tab and when **All** is selected in the Symbology field, **Enable** and **Strip Code ID** on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.*

When **All** is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

*Note: In Custom mode on the Data Options tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as Code IDs.*

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop down box, so the user can tell which symbologies have been modified from their defaults.

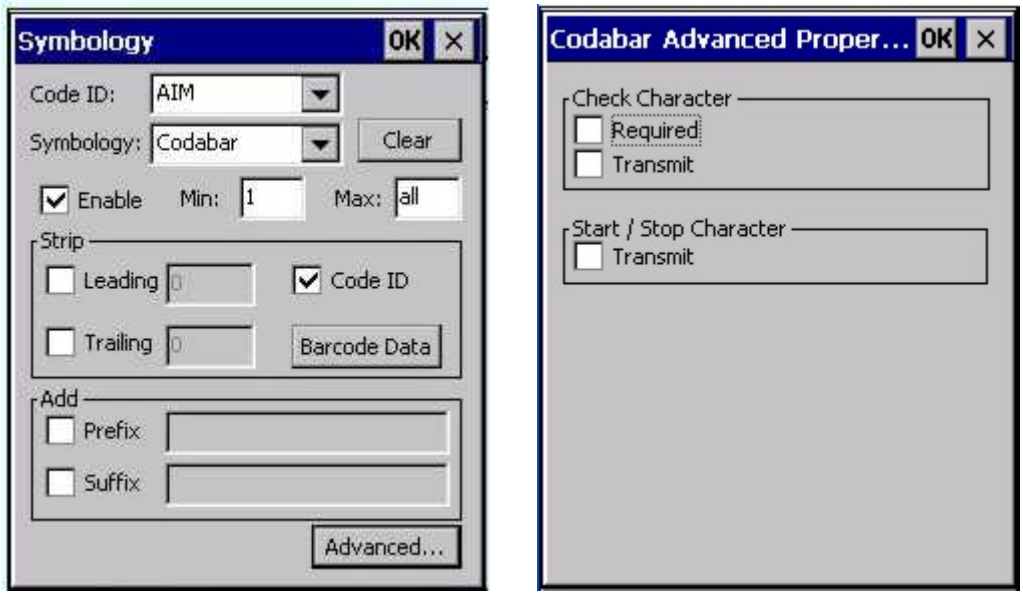
If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for **All** are used which is not necessarily the default.

Advanced Button

If there are advanced configuration options for the selected symbology, an Advanced button is displayed in the lower right corner of the panel. Not all barcode symbologies have configuration parameters so the Advanced button is not present for all symbologies.

Because the HHP imager does not support configuration barcodes, the Advanced function allows configuration parameters to be set for many of the supported barcodes.



The Symbology drop down box contains all symbologies **supported by the device selected on the Main tab**. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the OK button is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop down list.

Clear Button

Clicking this button will erase any programmed overrides, returning to the default settings for the selected symbology.

If **Clear** is pressed when **All** is selected as the symbology, a confirmation dialog appears:

then all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

Click the Yes button or the No button.

Enable, Min, Max

Enable

This checkbox enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the barcode data for the type of ID specified in the Data Options tab -- Enable Code ID field plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming barcode data, if the symbology is disabled, the barcode is rejected. Otherwise, the other settings in the dialog are applied and the barcode is processed.

If the symbology is disabled, all other fields on this dialog are dimmed.

If there ***are*** *customized settings*, uncheck the Enable checkbox for the All symbology. This results in disabling all symbologies *except* the customized ones.

Min

This field specifies the minimum length that the barcode data (not including Code ID) must meet to be processed.

Any barcode scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

Max

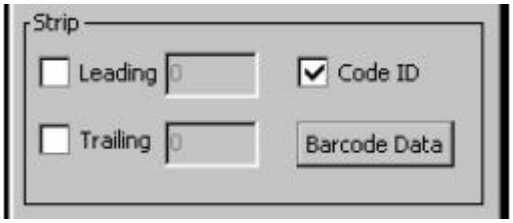
This field specifies the maximum length that the barcode data (not including Code ID) can be processed. Any barcode scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

Start | Settings | Control Panel | Data Collection | Data Options tab | Symbology button

This group of controls determines what data is removed from the collected data before the data is buffered for the application. When all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.



If the total number of characters being stripped is greater than the number of characters in the collected data, it becomes a zero byte data string.

If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading

This strips the number of characters specified from the beginning of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

This strips the number of characters specified from the end of the collected data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

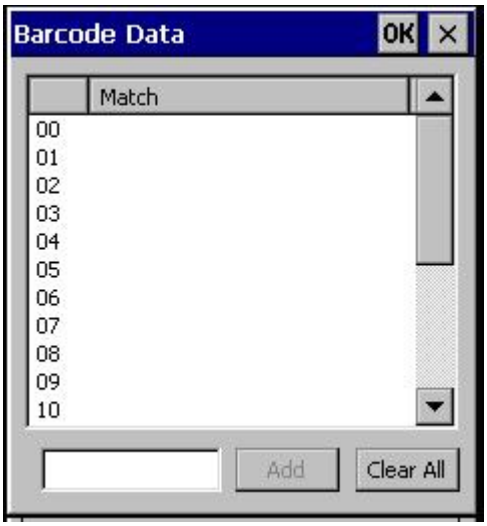
Code ID

Strips the Code ID based on the type code ID specified in the Enable Code ID field in the Data Options tab. By default, Code ID stripping is enabled for every symbology (meaning code IDs will be stripped, unless specifically configured otherwise).

Barcode Data Match List

Barcode Data Panel

This panel is used to strip data that matches the entry in the Match list from the barcode. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.



To remove an entry from the Match list, highlight the entry in the list and click the Remove button.

Click the OK button to store any additions, deletions or changes.

Barcode Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Click the **Add** button and the data is added to the next empty location in the Custom ID list.
Insert	Click on an empty line in the Custom ID list. The **Add** button changes to **Insert**. Enter data into both the Name and ID Code fields and click the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double click on the item to edit. Its values are copied to the text boxes for editing. The **Add** button changes to **Replace**. When Replace is clicked, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, clicking the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The **Clear All** button changes to a **Remove** button when an item in the Custom IDs list is selected. Click the desired line item and then click the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- **Prefix** and **Suffix** data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length barcode, a good beep will still be emitted, since barcode data was read from the scanner.

Match List Rules

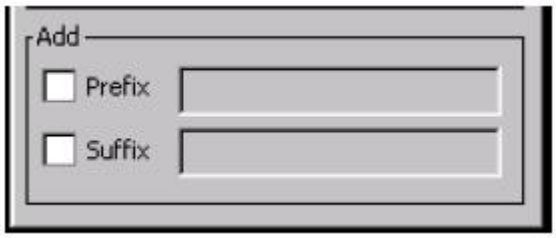
The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains ***ABC*** and ***AB***, in that order, incoming data with ***ABC*** will match first, and the ***AB*** will have no effect.
- When a match between the first characters of the barcode and a string from the list is found, that string is stripped from the barcode data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard * is not specified, the string is assumed to strip from the beginning of the barcode data. The string ***ABC**** strips off the prefix ***ABC***. The string ****XYZ*** will strip off the suffix ***XYZ***. The string ***ABC*XYZ*** will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)
- The question mark wildcard ***?*** may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The data collected is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of **Strip: Code ID** in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the barcode data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the barcode data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

Start | Settings | Control Panel | Data Collection | Symbology button

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the barcode data.



Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see *Hat Encoding* for a list of characters with their hex and hat-encoded values.

Use the **Escape** function to enter literal hex and hat values.

Add Prefix	To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the prefix is added for any symbology that has not been specifically configured.
Add Suffix	To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Suffix string is sent to the output buffer after the barcode data. Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the suffix is added for any symbology that has not been specifically configured.

Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g. F1), arrow keys, Page up, Page down, Home, and End.

Symbologies

There are three ID types. When an HHP imager scan engine is installed, only AIM, Custom and HHP ID Types are displayed. HHP does not support Symbol IDs.

When a Symbol scan engine is installed, AIM, Custom and Symbol are displayed as the ID Types. Symbol does not support HHP IDs.

Custom AIM IDs

Advanced properties are available when an integrated HHP imager is installed in the MX9. Advanced properties are applicable regardless of the ID type selected (AIM or HHP).

Not all HHP symbologies have Advanced options. Click the symbology link in the table below for symbology Advanced options.

Note: When the integrated scan engine is a Symbol scan engine, AIM IDs apply, but Advanced properties do not.

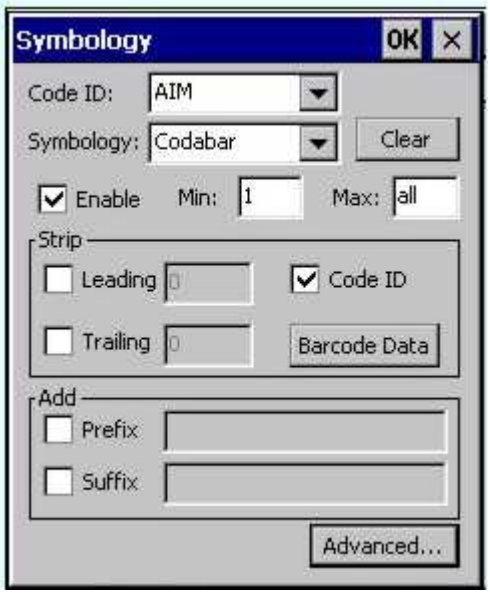
Factory Default settings

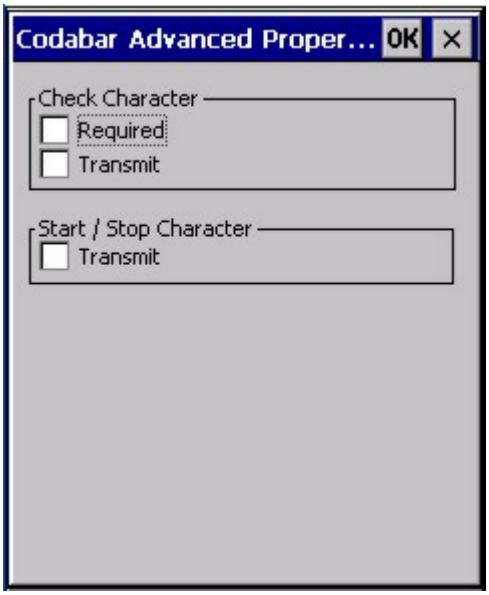
Symbology	Enabled?	Min	Max
All	Yes	1	all
Codabar	No	1	all
Code11	No	1	all
Code 39	No	1	all
Code 93	No	1	all
Code 128	Yes	1	all
Discrete 2 of 5	Yes	1	all
EAN 128	Yes	1	all
Interleaved 2 of 5	No	1	all
MSI	No	4	48
Other	Yes	1	all
PDF417	No	1	all
Plessey	No	4	48
RSS14	No	1	all
UPC/EAN	Yes	1	all

DCWedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

Codabar - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | AIM ID

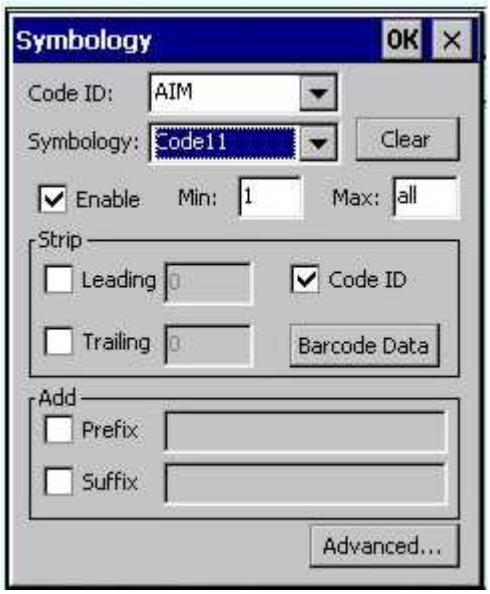


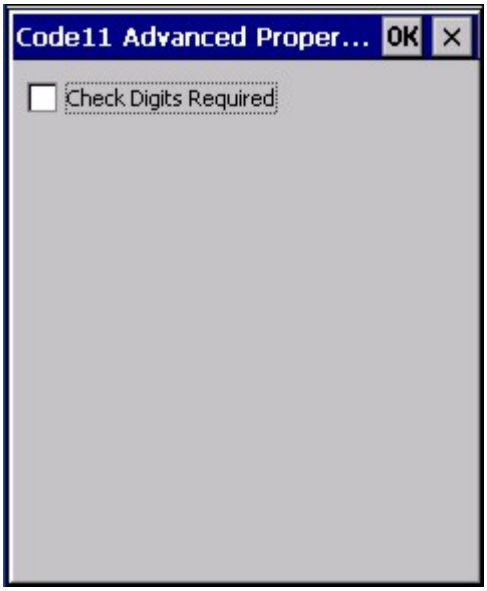


Option	Default Value
Check Character	Required : Disabled Transmit : Disabled
Start / Stop Character	Transmit : Disabled

Code11 - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | AIM ID

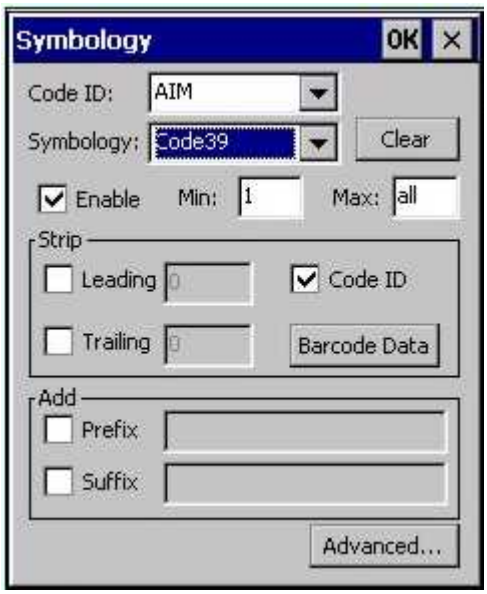


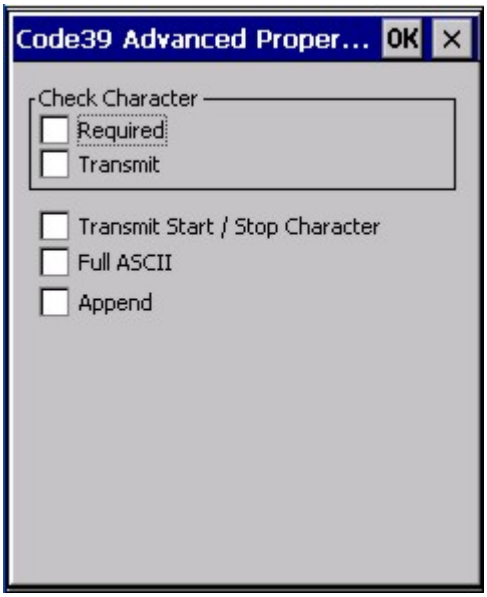


Option	Default Value
Check Digits Required	Required : Disabled

Code39 - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | AIM ID

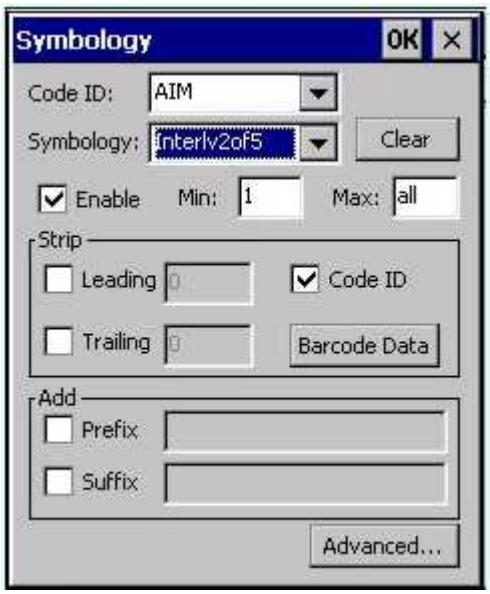


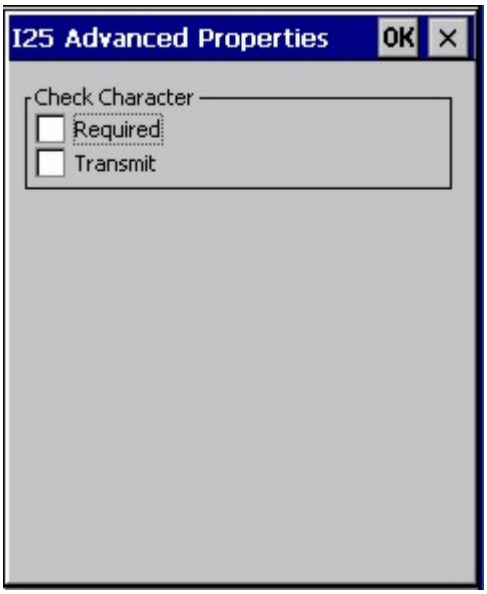


Option	Default Value
Check Character	Required : Disabled Transmit : Disabled
Start / Stop Character	Transmit : Disabled
Full ASCII	Disabled
Append	Disabled

Interleaved 2 of 5 - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | AIM ID

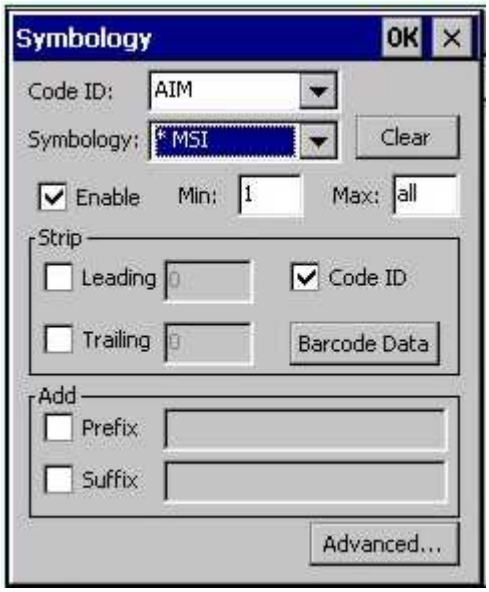


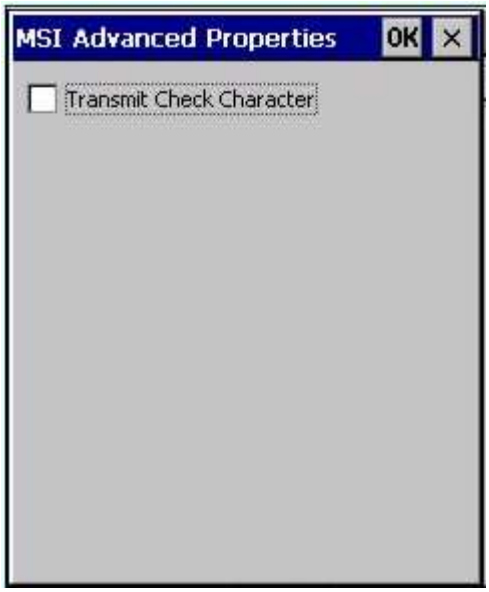


Option	Default Value
Check Character	Required : Disabled Transmit : Disabled

MSI - Advanced Properties

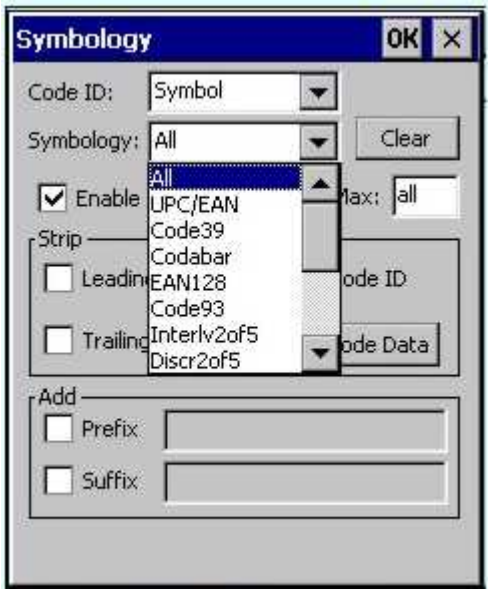
Start | Settings | Control Panel | Data Collection | Data Options | AIM ID





Option	Default Value
Transmit Check Character	Disabled

Custom Code IDs - Symbol



Symbol Custom Code IDs do not have Advanced options.

Factory Default settings

Symbology	Enabled?	Min	Max
All	Yes	1	all

HHP Custom IDs

Not all symbologies have Advanced options. Click the symbology link in the table below for symbology Advanced options.

Factory Default settings

*Note: **RSS and Composite**: Do not enable RSS and Composite at the same time. When they are both enabled, Composite overrides the RSS setting. Disable RSS when Composite is to be enabled, and disable Composite when RSS is to be enabled. The default setting for both is Disabled.*

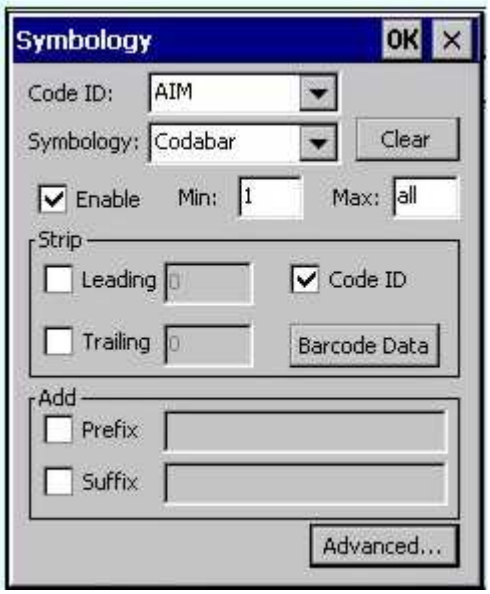
Symbology	Enabled?	Min	Max
All	Yes	1	all
Aztec	Yes	1	3750
BPO	No	1	all
Codabar	Yes	4	60
CodaBlock	No	0	2048
Code 11	No	4	80
Code 32	Yes	1	all
Code 39	Yes	0	48
Code 49	Yes	1	81
Code 93	Yes	0	80
Code 128	Yes	0	80
Composite	No	1	300
Coupon	No	1	all
DataMatrix	Yes	1	1500
EAN8	Yes	1	all
EAN13	Yes	1	all
EAN128	Yes	0	80
GenCode128	Yes	0	80
IATA25	No	4	80
IDTag	No	1	all
Interleaved 2 of 5	Yes	4	80
ISBT-1	No	1	all
Matrix 2 of 5	No	4	80
Maxicode	Yes	1	150
Mesa	Yes	1	all
MicroPDF	Yes	1	366
MSI	No	4	48

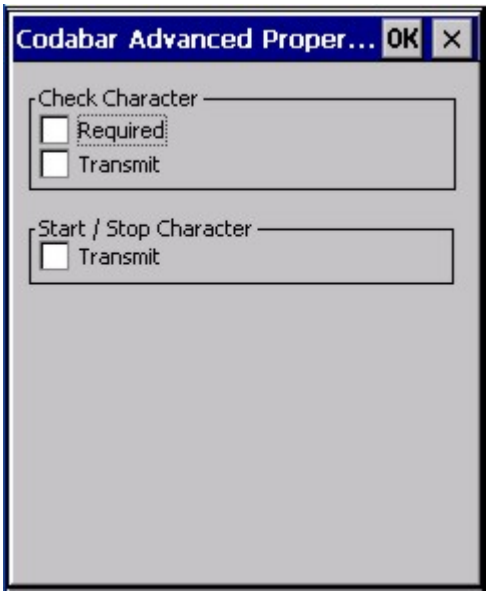
Symbology	Enabled?	Min	Max
OCR	No	1	all
Other	Yes	1	all
PDF417	Yes	1	2750
Plessey	No	4	48
Posi	No	4	48
Postnet	No	1	all
QR	Yes	1	3500
RSS	No	4	74
Strt25	No	4	48
Strt32	Yes	1	all
Telepen	No	1	60
TLC	No	1	all
Trioptic39	No	1	all
UPCA	Yes	1	all
UPCE0	Yes	1	all
UPCE1	Yes	1	al
CANPOST	No	1	all
AUSPOST	No	1	all
JapanPost	No	1	all
KoreanPost	No	4	48
Planet	No	1	all
DutchPost	No	1	all
ChinaPost	No	4	80
Code16K	No	1	160
Usps4cb	No	1	all

DCWedge does not manage mutually exclusive option selections. The user is responsible for understanding the options that can co-exist for the data collection device. The documentation provided from the manufacturer of the scanner/imager being managed describes the interaction between symbologies and their configurations.

Codabar - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

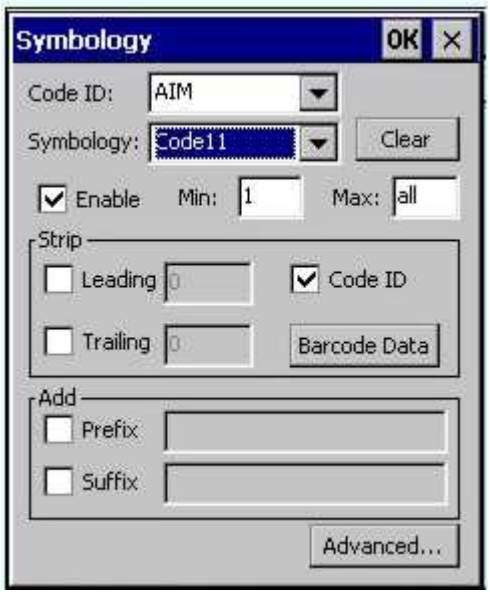


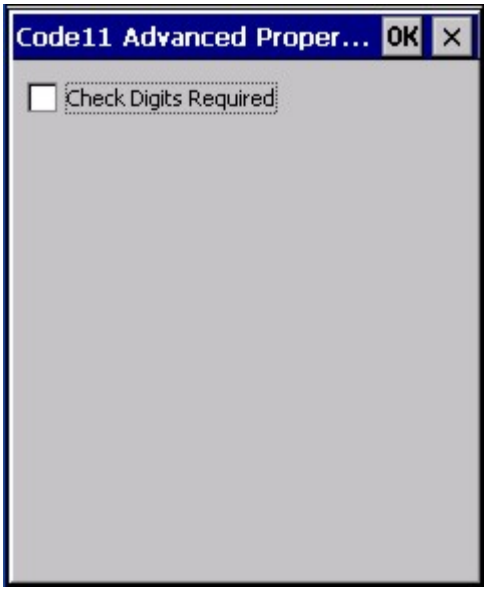


Option	Default Value
Check Character	Required : Disabled Transmit : Disabled
Start / Stop Character	Transmit : Disabled

Code11 - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

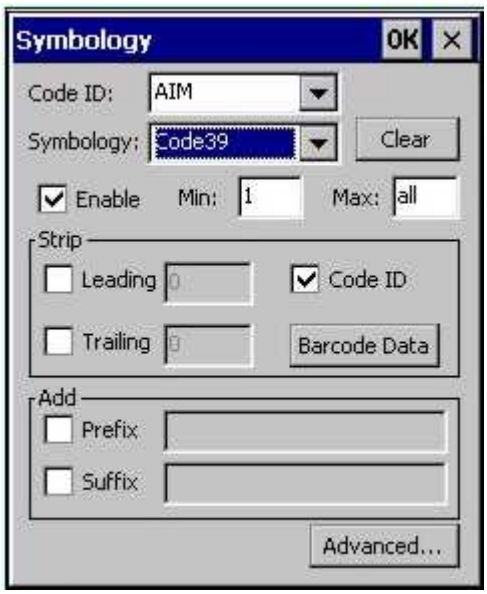


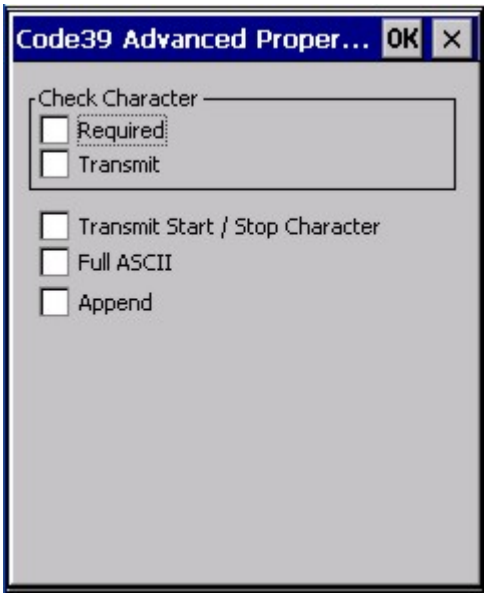


Option	Default Value
Check Digits Required	Required : Disabled

Code39 - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

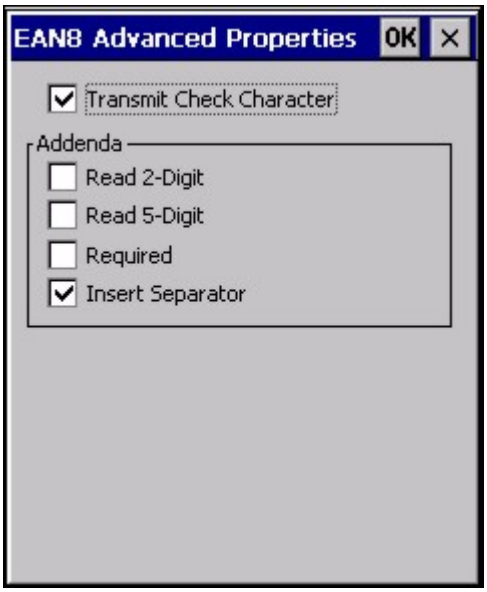




Option	Default Value
Check Character	Required : Disabled Transmit : Disabled
Start / Stop Character	Transmit : Disabled
Full ASCII	Disabled
Append	Disabled

EAN8 - Advanced Properties

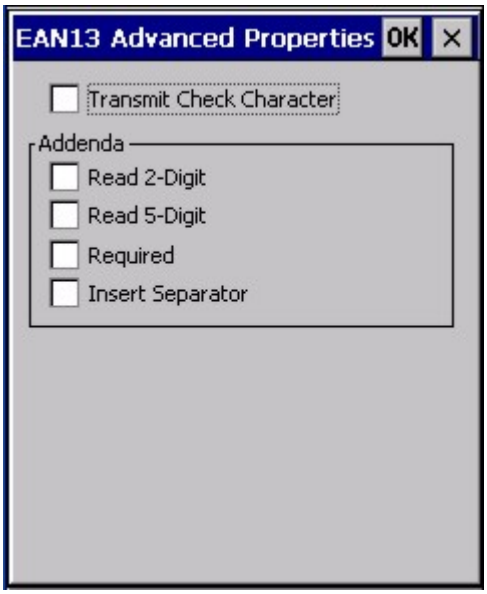
Start | Settings | Control Panel | Data Collection | Data Options | HHP ID



Option	Default Value
Transmit Check Character	Enabled
Read 2-Digit	Disabled
Read 5-Digit	Disabled
Required	Disabled
Insert Separator	Enabled

EAN13 - Advanced Properties

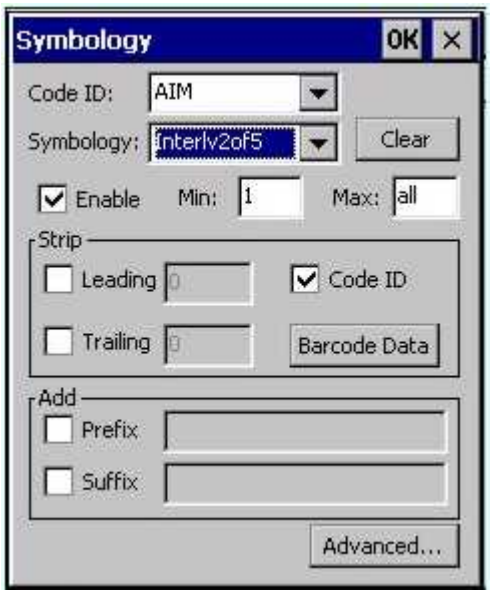
Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

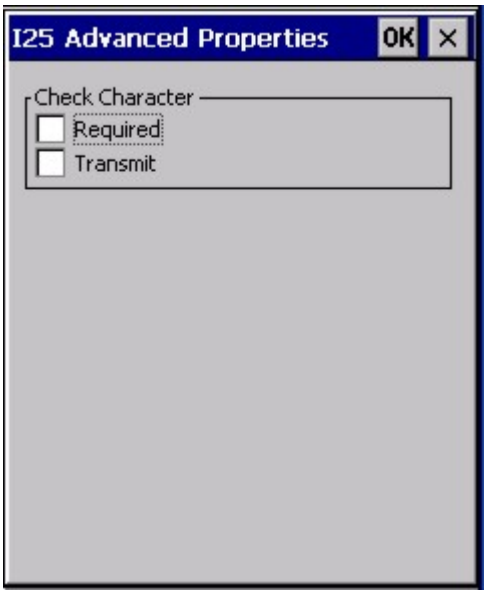


Option	Default Value
Transmit Check Character	Enabled
Read 2-Digit	Disabled
Read 5-Digit	Disabled
Required	Disabled
Insert Separator	Enabled

Interleaved 2 of 5 - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

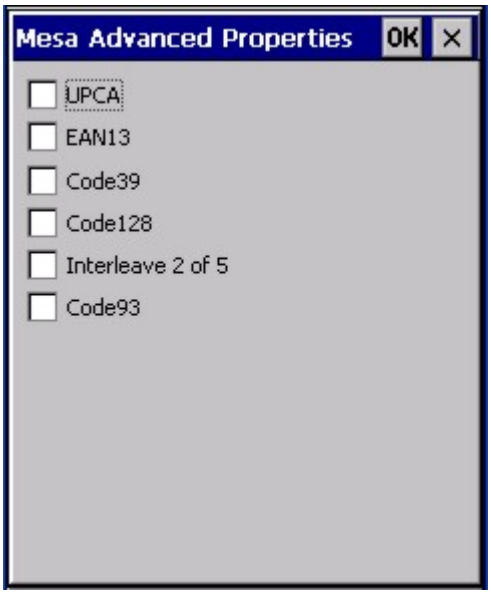




Option	Default Value
Check Character	Required : Disabled Transmit : Disabled

Mesa - Advanced Properties

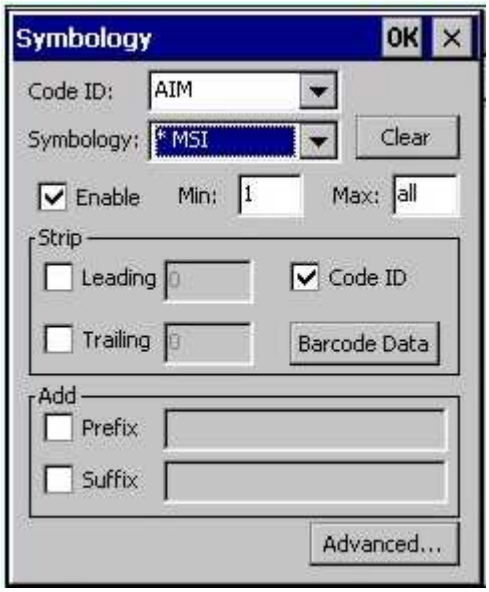
Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

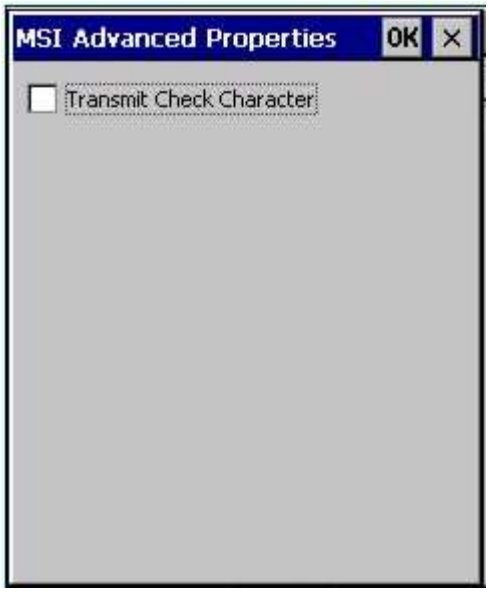


Option	Default Value
UPCA	Disabled
EAN13	Disabled
Code39	Disabled
Code128	Disabled
Interleaved 2 of 5	Disabled
Code93	Disabled

MSI - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

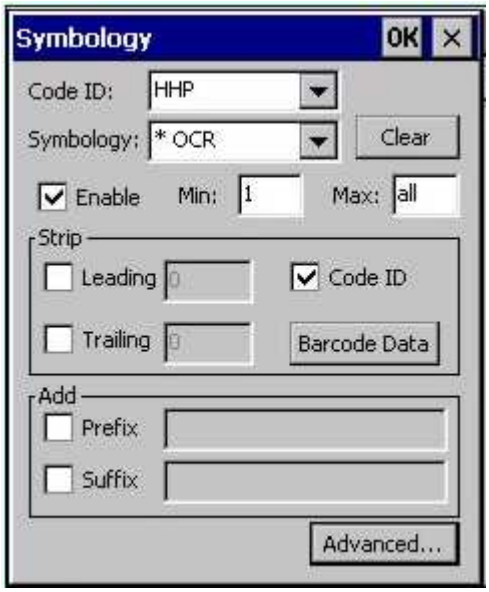




Option	Default Value
Transmit Check Character	Disabled

OCR Properties - Advanced

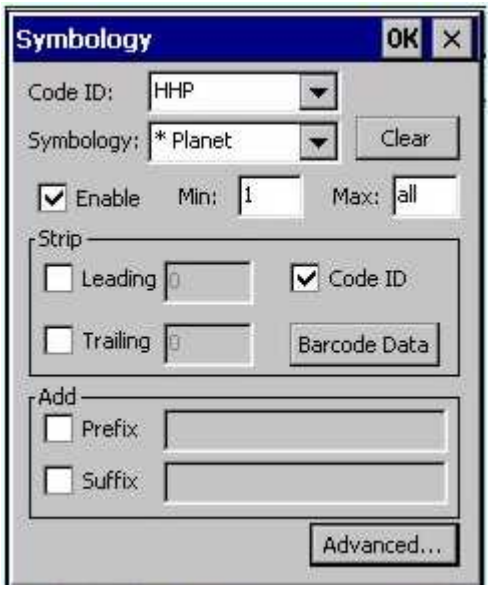
Start | Settings | Control Panel | Data Collection | Data Options | AIMHHPSymbol ID

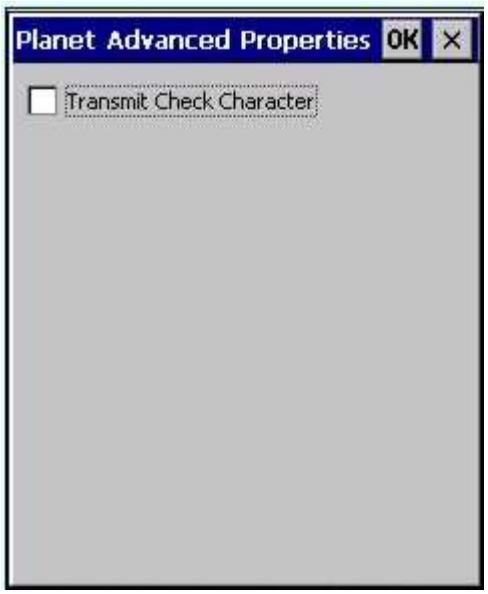


Option	Default Value
Font	Disabled
Direction	Left to Right
Template	dddddddd
Group G	Blank
Group H	Blank
Check	Blank

Planet - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | AIMHHPSymbol ID

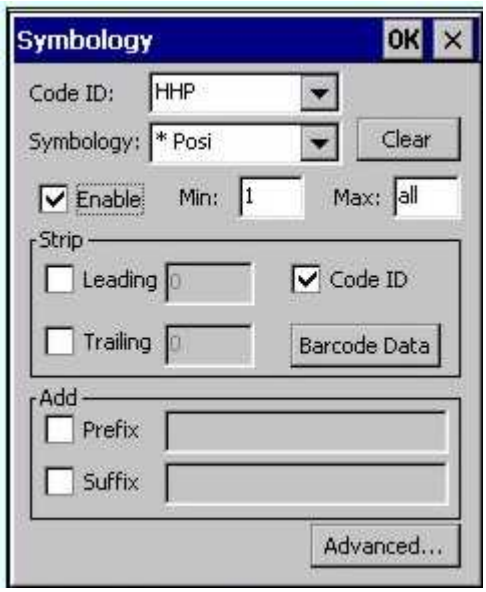


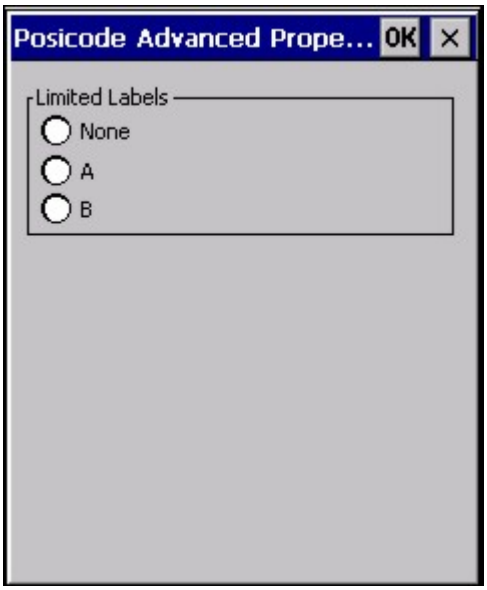


Option	Default Value
Transmit Check Character	Disabled

Posicode - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

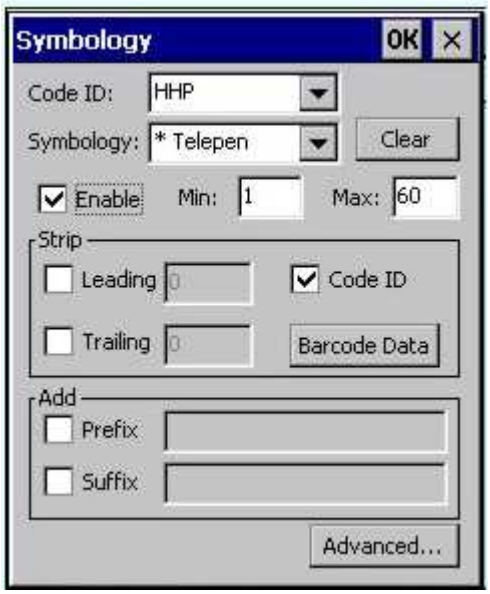


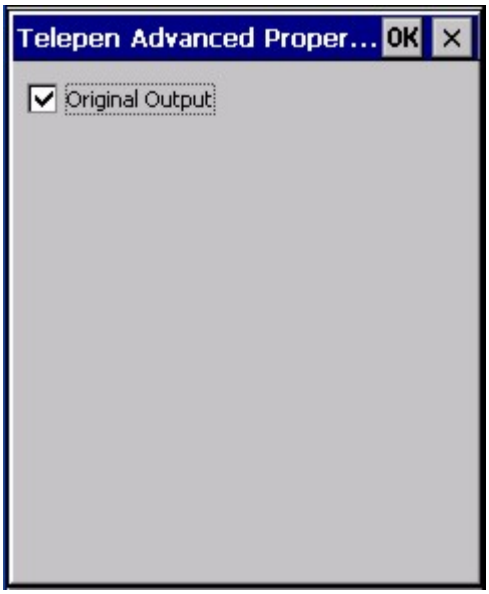


Option	Default Value
Limited Labels - None	Disabled
Limited Labels - A	Disabled
Limited Labels - B	Disabled

Telepen - Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | AIMHHPSymbol ID

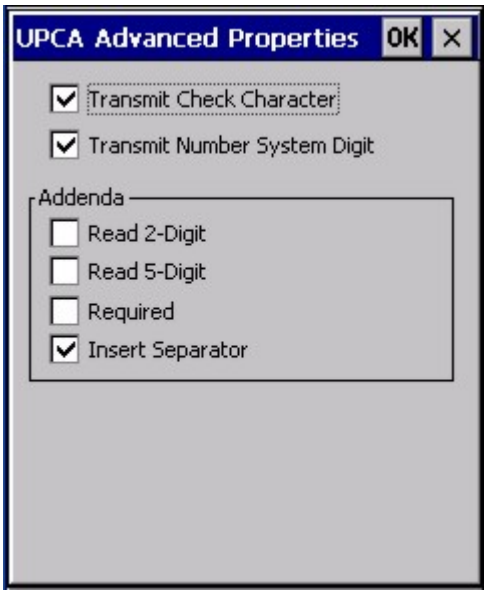




Option	Default Value
Original Output	Enabled

UPCA- Advanced Properties

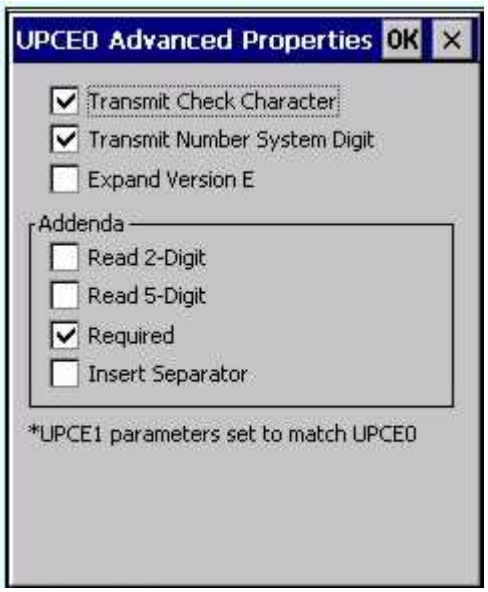
Start | Settings | Control Panel | Data Collection | Data Options | HHP ID



Option	Default Value
Transmit Check Character	Enabled
Transmit Number System Digit	Enabled
Addenda - Read 2-digit	Disabled
Addenda - Read 5-digit	Disabled
Addenda - Required	Disabled
Insert Separator	Enabled

UPCE0- Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

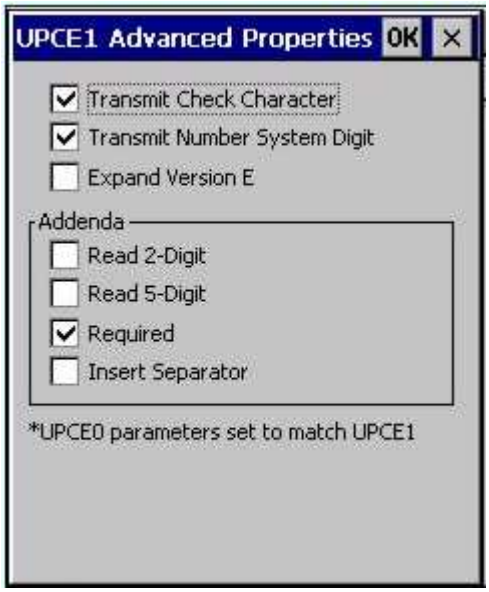


- For a device with an HHP integrated scanner, UPCE0 and UPCE1 are enabled as the same symbology at the scanner; therefore the only way for the UPCE1 configuration to be used is if UPCE0 is disabled. When UPCE0 is disabled, it will be scanned by the scanner, but rejected by DCWedge.
- The UPCE0 and UPCE1 parameters are always set to match each other. Therefore if a change is made to a parameter to either the EPCE0 or UPCE1 Advanced Properties that same change is automatically made to the Advanced Properties for the other symbology.

Option	Default Value
Transmit Check Character	Enabled
Transmit Number System Digit	Enabled
Expand Version E	Disabled
Addenda - Read 2-digit	Disabled
Addenda - Read 5-digit	Disabled
Addenda - Required	Enabled
Insert Separator	Disabled

UPCE1- Advanced Properties

Start | Settings | Control Panel | Data Collection | Data Options | HHP ID

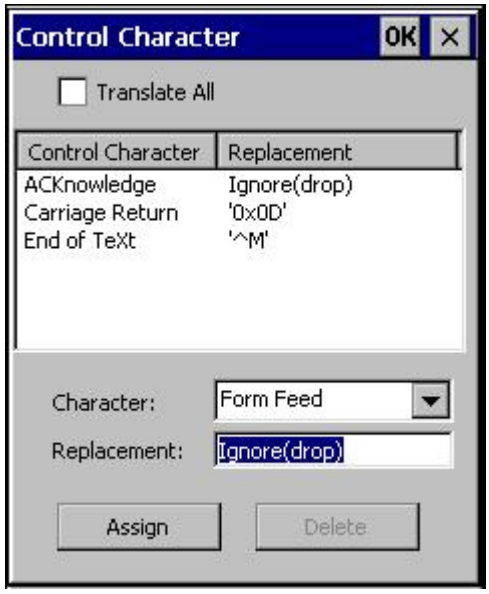


- For a device with an HHP integrated scanner, UPCE0 and UPCE1 are enabled as the same symbology at the scanner; therefore the only way for the UPCE1 configuration to be used is if UPCE0 is disabled. When UPCE0 is disabled, it will be scanned by the scanner, but rejected by DCWedge.
- The UPCE0 and UPCE1 parameters are always set to match each other. Therefore if a change is made to a parameter to either the EPCE0 or UPCE1 Advanced Properties that same change is automatically made to the Advanced Properties for the other symbology.

Option	Default Value
Transmit Check Character	Enabled
Transmit Number System Digit	Enabled
Expand Version E	Disabled
Addenda - Read 2-digit	Disabled
Addenda - Read 5-digit	Disabled
Addenda - Required	Enabled
Insert Separator	Disabled

Ctrl Char Mapping

The Ctrl Char Mapping button (Control Character Mapping) activates a dialog to define the operations the Data Collection Wedge performs on control characters (values less than 0x20) embedded in barcodes.



Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values.

In key message mode, control characters can also be translated to their control code equivalent key sequences.

Translate All

When **Translate All is checked**, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

Parameters

Translate All

This option is grayed unless the user has Send Key Messages (WEDGE) on the Main tab selected.

In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent control key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad).

Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke.

Any control code without a keystroke equivalent is dropped.

Character

This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names.

When a character name is selected from the drop down box, the default text *Ignore (drop)* is shown and highlighted in the Replacement edit control. *Ignore (drop)* is highlighted so the user can type a replacement if the control character is not to be ignored.

Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default *Ignore (drop)* in the Replacement edit control.

Replacement

The edit control where the user types the characters to be assigned as the replacement of the control character.

Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then clicking the button. The assigned replacement is then added to the list box above the Assign button.

For example, if Carriage Return is replaced by Line Feed (by specifying ^J or 0x0A) in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a.

The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

List Box

The list box shows all user-defined control characters and their assigned replacements.

All replacements are enclosed in single quotes to delimit white space that has been assigned.

Assign Button

Click this button when you want to assign the characters in the Replacement text box to the character in the Character drop down box.

Delete Button

This button is grayed unless an entry in the list box is highlighted.

When an entry (or entries) is highlighted, and the Delete button is clicked, the highlighted material is deleted from the list box.

Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for barcodes that do not use the standard AIM IDs, HHP IDs or Symbol IDs or for barcodes that have data embedded at the beginning of the data that acts like a Code ID.

These are called **custom Code IDs** and are included in the Symbology drop down box in the Symbology dialog, unless **Enable Code ID** is set to **None**. When the custom Code ID is found in a barcode, the configuration specified for the custom Code ID is applied to the barcode data.

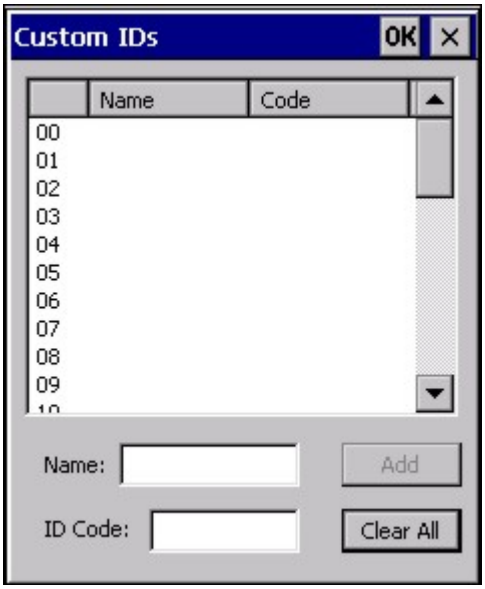
It is intended that custom code IDs are used to supplement the list of standard code IDs (if **Enable Code ID** is set to **AIM, Symbol** or **HHP**), or to replace the list of standard code IDs (if **Enable Code ID** is set to **Custom).**

When **Enable Code ID** is set to **None**, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

*Note: When **Strip: Code ID** is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).*

The dialog box shown below allows the custom Code IDs to be configured. When incoming data is checked for a custom ID code, the list is compared in the order displayed in this dialog box.



After adding, changing and removing items from the Custom IDs list, click the OK button to save changes and return to the Barcode panel.

Parameters

Name text box

Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the Name and ID Code may have the same value. Name is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box

ID Code defines the data at the beginning of a barcode that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

Add

Entering data into both the Name and ID Code fields enables the Add button. Click the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Click on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and click the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double click on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is clicked, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, clicking the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button text changes to a Remove button when an item in the Custom IDs list is selected. Click the desired line item and then click the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration Data	Translation	Example Control Character	Example Configuration	Translated Data
Ignore (drop)	The control character is discarded from the barcode data, prefix and suffix	ESCape	Ignore (drop)	0x1B in the barcode is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	STX	0x02 in a barcode is converted to the text STX.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	^M	Value 0x0d in a barcode is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass through to the application.	Horizontal Tab	\^I	Value 0x09 in a barcode is converted to the text ^I.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	0x0A	Value 0x0D in a barcode is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass through to the application.	Vertical Tab	\0x0A or 0\x0A	Value 0x0C is a barcode is converted to text 0x0A

See "Hat Encoding" on page 284

Barcode Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit an AIM identifier.

	Symbology				
	All	**EAN-128(]C1)**	**EAN-13(]E0)**	**Intrlv 2 of 5(]I0)**	**Code93**
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		*123	1*	456	
Strip Trailing	0	0	3	3	
Prefix	aaa	bbb	ccc	ddd	
Suffix	www	xxx	yyy	zzz	

Provided that the wedge is configured with the above table, below are examples of scanned barcode data and results of these manipulations.

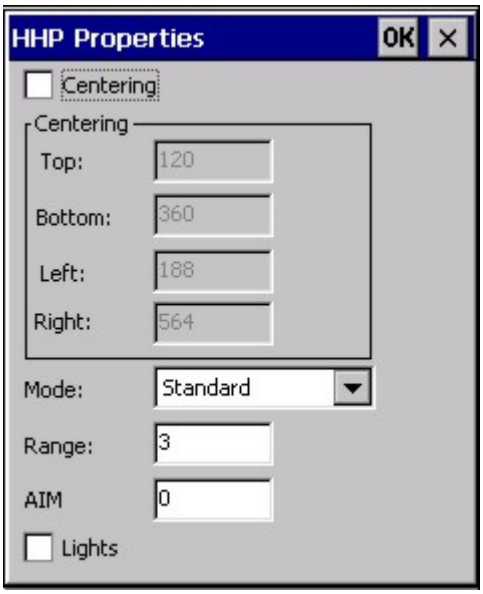
Barcode Symbology	Raw Scanner Data	Resulting Data
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	*< rejected > (too short)*
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	***< rejected >*** *(too long)*
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	***< rejected >*** *(disabled)*
Code-93	]G0444444	***< rejected >*** *(disabled)*
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	***< rejected >*** *(too short)*

Note: Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned barcode data by the processing causes a bad scan beep on the same data.

HHP Properties

Start | Settings | Control Panel | Data Collection | Data Options tab

Use these options to configure HHP imager parameters.



Centering default is Disabled.

Decode mode default is Standard.

Linear Range default is 3.

Aim Timer default is 0 (no time).

Imager's lights and aimer are disabled for the scan duration.

Centering

Start | Settings | Control Panel | Data Collection | HHP Properties button

The centering feature is used to allow the user to accurately scan a selected barcode among a group of barcodes that are located closely together. When centering is turned on, the imager will only decode barcodes that intersect the centering window defined by the user. The centering window must intersect the center of the barcode.

The default centering settings define a 60 pixel square area in the center of the imager's field of view.

Default centering settings and allowable minimum and maximum settings are listed below.

Centering	Enable
Default	0
Valid	1 Enable
	0 Disable

Enable or disable Centering feature. When disabled, the following values are ignored.

Position	Default	Minimum	Maximum
CenteringTop	120	0	239
CenteringBottom	360	240	479
CenteringLeft	188	0	319
CenteringRight	564	320	639

DecodeMode

Start | Settings | Control Panel | Data Collection | HHP Properties button

Default	1
Valid	1 = Normal mode
	2 = Aggressive Linear Decode (ALD)
	4 = Quick Omni

In Normal mode the imager will decode both linear and 2-D symbologies.

In Aggressive Linear Decode mode the imager will only read linear symbologies in this mode, but decoding these is faster and more accurate than Normal Mode.

In Quick Omni mode the imager searches for a barcode in a reduced field located around the center of the image. Decoding is faster in this mode, but the user must center the aiming line over the barcode to be read. Both linear and 2-D symbologies can be read in this mode.

LinearRange

Start | Settings | Control Panel | Data Collection | HHP Properties button

Default	3
Valid	1 - 6

1 specifies that the linear range that is searched for a readable label is a tight vertical range near the aimer.

6 specifies that the entire height of the image is to be searched.

AimTimer

Start | Settings | Control Panel | Data Collection | HHP Properties button

Duration of the imager aim beam in 0.1 second increments.

Default	0
Valid	0 = 50 (0 – 5 seconds)

If a value greater than 50 is entered, the aim duration is set to the maximum time of 5 seconds.

LeaveLightsOn

Start | Settings | Control Panel | Data Collection | HHP Properties button

Default	0
Valid	0 = Off, 1 = On

Specifies if the imager's lights and aimer should be left on during the entire decode process.

If Off, the lights are turned on only during image capture, then turned off while the imager attempts to process and decode the barcode.

If On, the aimer and lights remain turned on during the entire process.

In Aggressive Linear Decode mode, set this parameter to 1 to improve the aimer visibility.

About Tab

Start | Settings | Control Panel | Data Collection | About tab

This tab displays the Data Collection Wedge driver version installed in the MX9. The version number shown in the image below is used only as an example, your version number will be different.

It also lists the type of scanner/imager installed. Valid scanner / imager types are:

- HHP - Hand Held Products 53XX 2D Imager
- Symbol - Symbol laser scanner
- Blank - No integrated scanner

Length Based Barcode Stripping

Use this procedure to create symbology rules for two barcodes with the same symbology but with different discrete lengths. This procedure is not applicable for barcodes with variable lengths (falling between a maximum value and a minimum value).

Example 1:

- A normal AIM or Symbol symbology role can be created for the desired barcode ID.
- Next, a custom barcode symbology must be created using the same Code ID as the original AIM or Symbol ID rule and each rule would have unique length settings.

Example 2:

For the purposes of this example, the following sample barcode parameters will be used – EAN 128 and Code 128 barcodes. Some of the barcodes start with '00' and some start with '01'. The barcodes are different lengths.

- 34 character length with first two characters = "01" (strip first 2 and last 18)
- 26 character length with first two characters = "01" (strip first 2 and last 10)
- 24 character length with first two characters = "01" (strip first 2 and last 8). This 24 character barcode is Code 128.
- 20 character length with first two characters = "00" (strip first 0 (no characters) and last 4)

On the Data Options tab, set Enable Code ID to AIM.

Create four custom IDs, using 1 for EAN 128 barcode and 0 for Code 128 barcode.

- c1 = Code = ']C1'
- c2 = Code = ']C1'
- c3 = Code = ']C0' (24 character barcode is Code 128)
- c4 = Code = ']C1'

AIM custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = "01"
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = "01"
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = "01"
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = "00"

Add the AIM custom symbologies. Refer to the previous section *Symbology Settings* for instruction.

Click the Barcode Data button.

Click the Add button.

Add the data for the match codes.

Refer to the previous section *Barcode Data Match List* for instruction.

Scan a barcode and examine the result.

Date / Time

Start | Settings | Control Panel | Date/Time - or - Time in Desktop Taskbar

Use this MX9 panel to set Date, Time, Time Zone, and assign a Daylight Savings location.

Factory Default Settings

Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Enabled

Date/Time Properties
?
OK
Date/Time
January 2009
S M T W T F S
28 29 30 31 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
1 2 3 4 5 6 7
2:09:32 PM
Time Zone
(GMT-05:00) Eastern Time (US & C
Automatically adjust clock for daylight saving
Apply

There is very little functional change from general desktop or laptop Date/Time Properties options.

Double-tapping the time displayed in the Desktop Taskbar causes the Date/Time Properties screen to appear.

The Sync button activates a utility that will set the clock using a network time server.

Dialing

Start | Settings | Control Panel | Dialing

Set dialup properties for internal modems (not supplied or supported on the MX9 by LXE).

Factory Default Settings

Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled (blank)

Display

Start | Settings | Control Panel | Display

The display might also called the touchscreen.

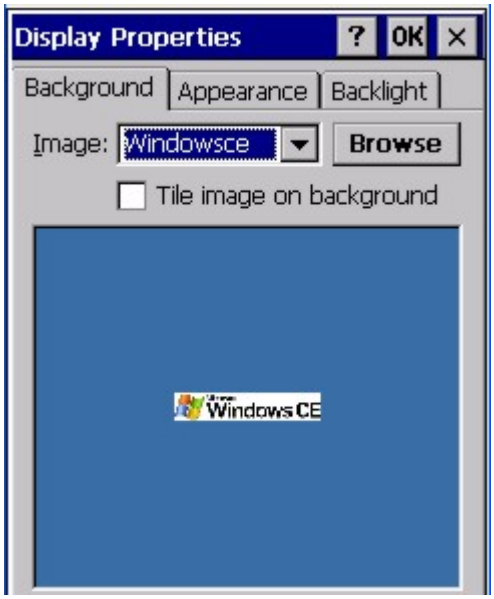
Select the desktop background image and appearance scheme for the MX9. Using the options on the Backlight tab, set the display backlight and keypad backlight timers when running on battery or external power.

Adjust the settings and tap the OK button to save the changes. Saved changes take effect immediately.

Factory Default Settings

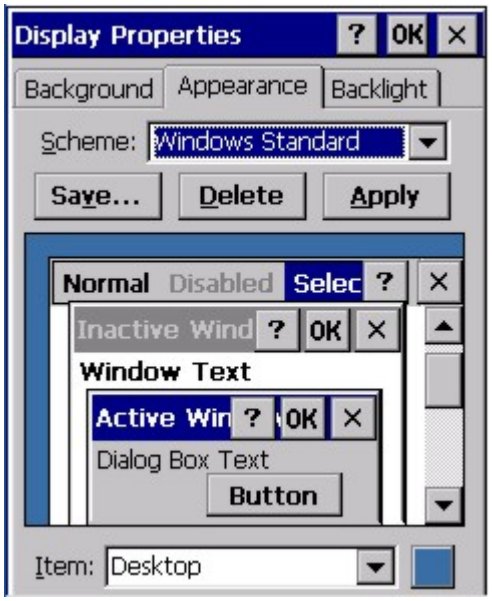
Background	
Image	Windows CE
Image on background	Disabled
Appearance	
Schemes (color displays)	Windows Standard
Schemes (monochrome displays)	High Contrast White
Backlight	
Battery power and user idle	3 seconds
Battery power and System idle	15 seconds
Battery power, idle, Suspend	5 minutes
External power and user idle	2 minutes
External power and System idle	2 minutes
External power, idle, Suspend	2 minutes
Backlight Brightness	Maximum

Background



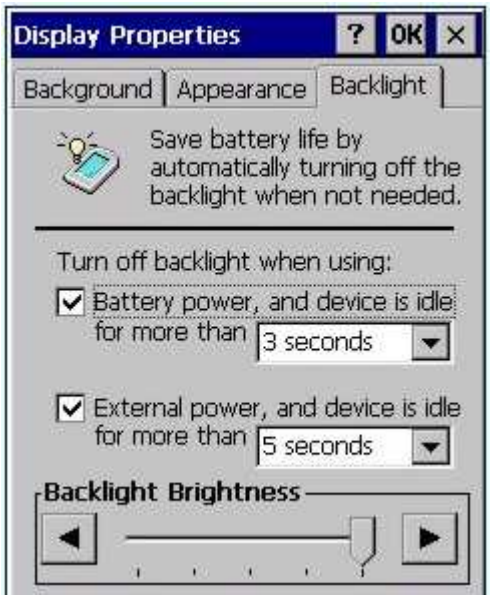
There is very little change from general desktop PC Display Properties / Background options. Select an image from the drop down list (or tap the Browse button to select an image from another folder) to display on the Desktop, and then tap the OK button to save the change. The change takes effect immediately.

Appearance



There is very little change from general desktop PC Appearance options. Select a scheme from the drop down list and make changes to the parameters. The default is High Contrast White for monochrome displays and Windows Standard for color displays. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the display.

Backlight



The backlight settings use the LXE set of default timeouts and is synchronized to the User Idle setting in the Schemes tab in the Power control panel. When the backlight timer expires, the touchscreen backlight is dimmed, not turned off. When both

checkboxes are unchecked, the backlight never turns off (or dims). Default values are 3 seconds for Battery, 2 minutes for External and both the check boxes are enabled.

When the **keypad backlight** is set to *Follow the touchscreen backlight*, the keypad backlight turns off when the touchscreen backlight dims.

Adjust **backlight brightness** by moving the slider. Changes are in effect immediately.

Touchscreen display backlight brightness **adjust mode** is entered by pressing the **Blue + Scan** key combination.

After this, the up and down arrow keys brighten or dim the backlight. Pressing any key other than up arrow or down arrow exits the brightness adjustment mode.

Additional characteristics:

- There is no separate brightness level indication except for the actual brightness of the display.
- Once the maximum (or minimum) brightness is reached by repeated presses of the up (or down) key, the display will cease getting brighter (or dimmer) and saturate at that maximum (or minimum brightness).
- Continuously pressing the up or down arrow keys does not cause an automatic repeat of the up (or down) arrow key.
- The brightness setting is stored in the registry and is recalled at power on.
- The number of steps from maximum brightness to minimum dimness is five. At minimum dimness level, the display is still viewable.

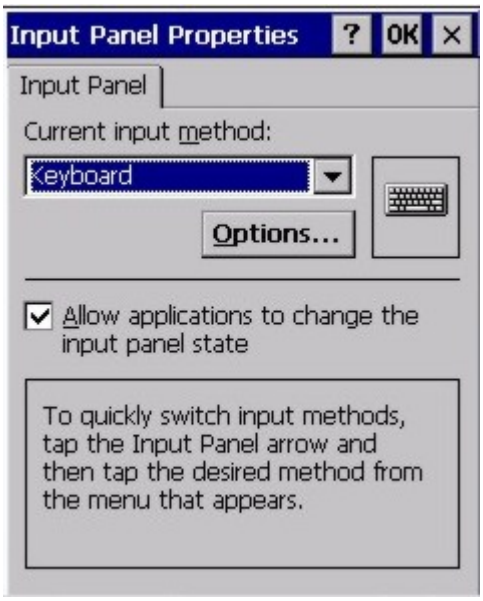
Input Panel

Start | Settings | Control Panel | Input Panel

Set the current MX9 keys and data input method.

Factory Default Settings

Input Method	Keyboard
Allow applications to change input panel state	Enabled
Options button	
Keys	Small keys
Use gestures	Disabled


Input Panel Properties
?
OK
Input Panel
Current input method:
Keyboard
Options...
Allow applications to change the input panel state
To quickly switch input methods, tap the Input Panel arrow and then tap the desired method from the menu that appears.

Use this panel to make the Input Panel (on-screen keyboard) or the physical keypad primarily available when entering data on any screen.

Selecting **Keyboard** enables both.

Tap the Options button to set the size of the keys displayed on-screen and whether Transcriber gestures are enabled or disabled.

Note: Contact your LXE representative for language packs as they become available.

Internet Options

Start | Settings | Control Panel | Internet Options

Set options for MX9 Internet connectivity. Select a tab. Tap the ? button for help using Windows CE Help installed in your mobile device. Adjust the settings and tap the OK button. The changes take effect immediately.

Factory Default Settings

General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Bypass Proxy	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Privacy	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced	
Stylesheets	Enabled
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

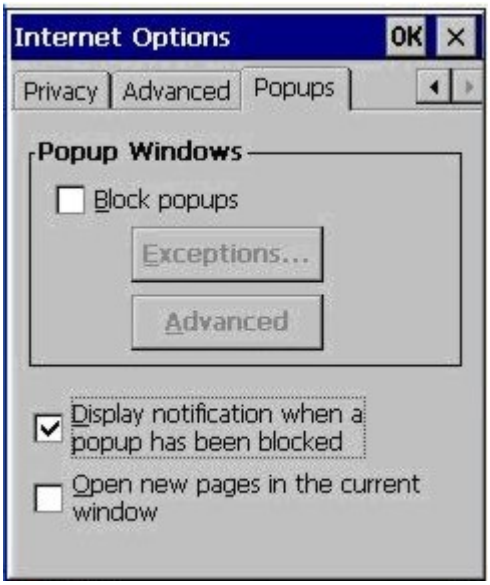
Internet Options
OK
General
Connection
Security
Start Page:
http://www.lxe.com
Search Page:
http://www.google.com
User Agent (requires browser restart):
Default (Windows CE)
Cache Size (in KB):
512
Clear Cache
Clear History

Internet Options
OK
General
Connection
Security
Use LAN (no autodial)
Autodial name:
USB Client
Network
Access the Internet using a proxy server
Address:
Port:
80
Bypass proxy server for local addresses

Internet Options
OK
General
Connection
Security
Internet
Local intranet
Trusted site
Internet
This zone contains all Web sites you haven't placed in other zones
Sites...
Settings...

Internet Options
OK
Connection
Security
Privacy
Cookies
First-party
Third-party
Accept
Block
Prompt
Accept
Block
Prompt
Always allow session cookies

Internet Options
OK
Security
Privacy
Advanced
Popu
Accessibility
Always expand ALT text for
Anchors navigate on access
Browsing
Always send URLs as UTF-8
Display a notification about e
Enable stylesheets
Enable page transitions
Theming support
Disable automatic SIP
Underline links
Never


Internet Options
OK
Privacy
Advanced
Popups
Popup Windows
Block popups
Exceptions...
Advanced
Display notification when a popup has been blocked
Open new pages in the current window

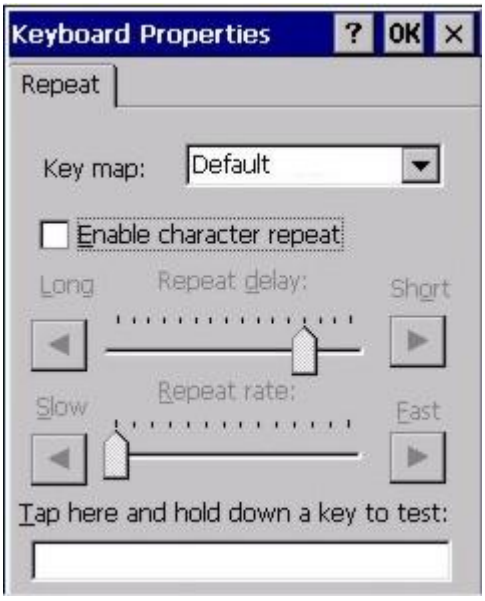
Keyboard

Start | Settings | Control Panel | Keyboard

Set keypad key map, keypad key repeat delay, and key repeat rate.

Factory Default Settings

Repeat Tab	
Key map	Default (or Default MX9)
Repeat character	Enable
Repeat Delay	Short
Repeat Rate	Slow



Select a key map using the drop down list. Adjust the character repeat settings and tap the OK button to save the changes.

When new key maps, or fonts, are added to the registry, they are available immediately and the font name is in the Keyboard Properties Key map drop down list. Only one font at a time can be selected. The fonts affect the screen display, they do not affect any virtual (touchscreen) key taps.

See **About | Software | Language** tab for the name of any installed fonts.

Languages and Fonts[1]

See Also: Regional Settings for instruction for setting User Interface Language and Default Input Language.

[1]Fonts are available in the following languages (in separate part numbers) for each language: Simplified Chinese, Traditional Chinese, Korean, Japanese.
Tahoma font is on every unit and includes English (default), European (French, Spanish, German, Portuguese), Scandinavian languages, Arabic, Cyrillic, Greek, Hebrew, and Thai.

KeyMap

Start | Settings | Control Panel | KeyMap Icon

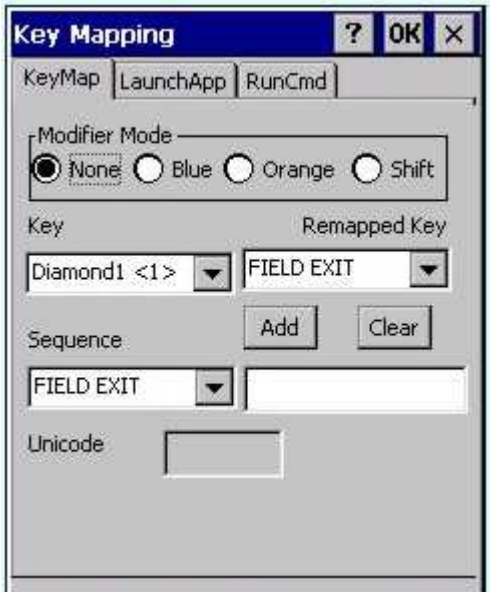
Use this control panel option to assign key functions to mappable keys available on your MX9, determine application launch sequences and program command Run sequences.

Note: KeyMap Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets. For example, the AppLock Administrator Control panel file Launch option.

Factory Default Values

KeyMap		
Modifier Mode	None	
Key	Diamond 1	Remap to – Field Exit
Edit String	Field Exit	String – Empty
LaunchApp		
App1	Empty	
App2	Empty	
App3	Empty	
App4	Empty	
App/Opt	EXE	
RunCmd		
Cmd1	Empty	
Cmd2	Empty	
Cmd3	Empty	
Cmd4	Empty	
File/Parm	FILE	

KeyMap Tab



Assign settings by clicking radio buttons and selecting keys from the drop down boxes. Tap the OK button when finished. The changes take effect immediately.

How to Remap a Single Key

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key drop down list.
3. Select the value from the remapped key from the Remapped Key drop down list.
4. Click OK to save the result and close the Keypad Control.

How to Remap a Key Sequence

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key drop down list.
3. Select Key Sequence from the Remapped Key drop down list.
4. Select the first key for the multiple key sequence from the drop down list. Press the Add button to add the key to the multiple key sequence shown in the Key Sequence box. Repeat this step until all keys desired have been added to the key sequence. If necessary, use the Clear button to erase all entries in the Key Sequence box.
5. Click OK to save the result and close the Keypad Control.

Note: A key can only be used once in a multiple key sequence. For example, an F1 key added to a key sequence means an F1 key cannot be used again in the same key sequence.

How to Remap an Application

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key drop down list.
3. Select Launch App1-4 from the remapped key from the Remapped Key drop down list.
4. Click on the LaunchApp tab.
5. Make sure the EXE radio button is selected.

6. In the text box (App1-4) corresponding to the number selected for Launch App1-4, enter the application to launch.
7. If any parameters are needed for the application, click on the OPT radio button. This clears the text box (though the application name is saved). Enter the desired parameters in the appropriate text box.
8. Click OK to save the result and close the Keypad Control.
9. If the KeyMap tab is accessed again, the application plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

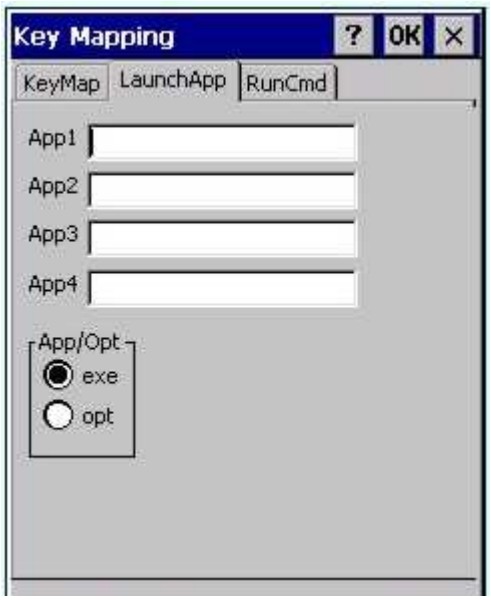
How to Remap a Command

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key drop down list.
3. Select RunCmd 1-4 from the remapped key from the Remapped Key drop down list.
4. Click on the RunCmd tab.
5. Make sure the FILE radio button is selected.
6. In the text box (Cmd1-4) corresponding to the number selected for RunCmd1-4, enter the desired command.
7. If any parameters are needed for the command, click on the PARM radio button. This clears the text box (though the command is saved). Enter the desired parameters in the appropriate text box.
8. Click OK to save the result and close the Keypad Control.
9. If the KeyMap tab is accessed again, the command plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

LaunchApp Tab

The default for all text boxes is Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the MX9 emits a single beep, if the launch is successful, it is silent.



The Launch App command is defined for use by system administrators. These instructions are parsed and executed directly by the keyboard driver.

1. Place the cursor in the text box next to the App you wish to run, e.g. App1, App2.
2. Enable the EXE radio button if the application is an EXE file.
3. Enter the name of the executable file.
4. Enable the OPT radio button to add options or parameters for the executable file in the same text box. Switching from EXE to OPT clears the text box (but the information previously entered is stored), allowing parameter entry.

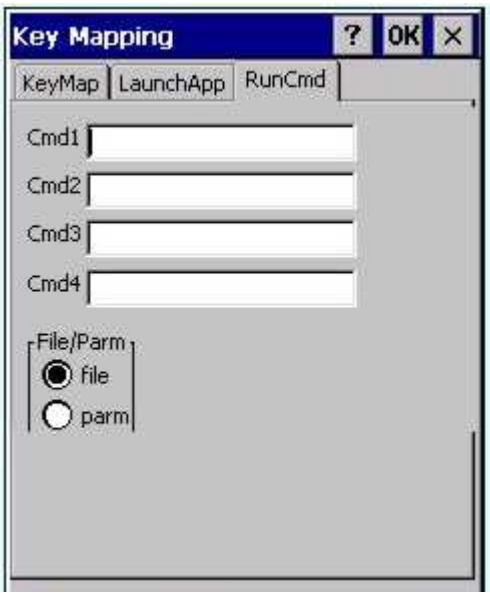
Tap the OK button when finished. The changes take effect immediately.

The result of the application (exe) and options (opt) entries are displayed on the KeyMap tab in the Key Sequence box when the key mapped to the LauchApp is selected.

RunCmd Tab

The default for all text boxes is Empty, Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the MX9 emits a single beep, if the launch is successful, the mobile device is silent.



The Run Cmd command is defined for use by system administrators. These instructions call the ShellExecuteEx API, which opens documents directly.

1. Place the cursor in the text box next to the Cmd you wish to run, e.g. Cmd1, Cmd2.
2. Enable the file radio button and enter the name of the file.
3. Enable the PARM radio button to add parameters for file/exe execution in the same text box.

Tap the OK button when finished. The changes take effect immediately.

Mixer

Start | Settings | Control Panel | Mixer

The MX9 has a speaker and a microphone. They are active when a headset is not connected to the device.

The microphone is located to the left of the LXE oval logo at the top of the unit.

The speaker (audio) is located above the keypad.

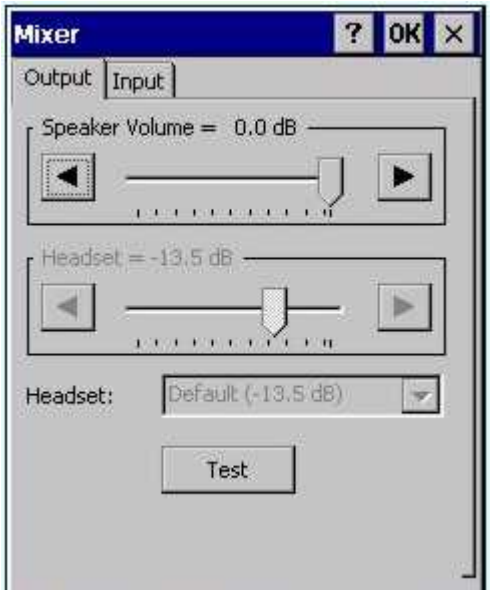
Use the settings on these panels to adjust the volume, record gain and sidetone for microphone input, speaker and speaker output.

Headsets can be enabled, disabled and selected using these panels.

Factory Default Settings

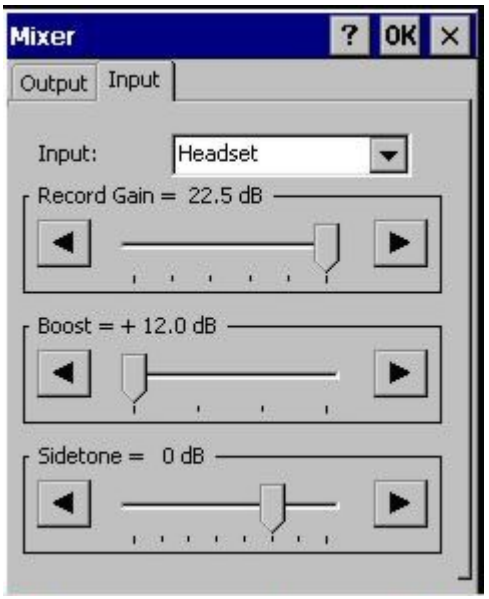
Output	
Speaker Volume	0 dB
Headset Volume	-13.5dB
Headset Selection	Default
Input	
Input Selection	None
Record Gain	0 dB
Record Boost	+12 dB
Sidetone	0 dB

Output panel



Tap and hold the Output sliders and move them either left or right, or tap the left and right arrows, to adjust Speaker volume decibel level. Tap the drop down list arrow to select the type of headset currently attached to the unit. This will load a predetermined limit value; the headphone setting cannot exceed the predetermined values.

Input Panel



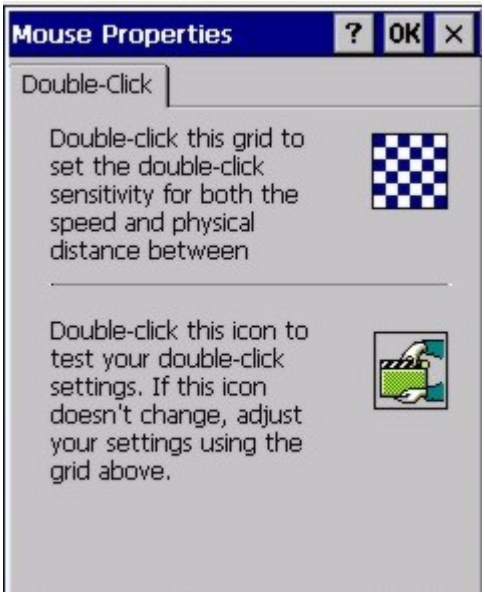
To enable the headset, select **Headset** in the Input Selection combo box. To disable the headset, select **None** in the Input Selection combo box.

Note: The list of input selections and headset selections is stored in the registry. Both WAN and Bluetooth are included in the input list in the registry, but with the disabled flag set, they do not appear in the list.

Mouse

Start | Settings | Control Panel | Mouse

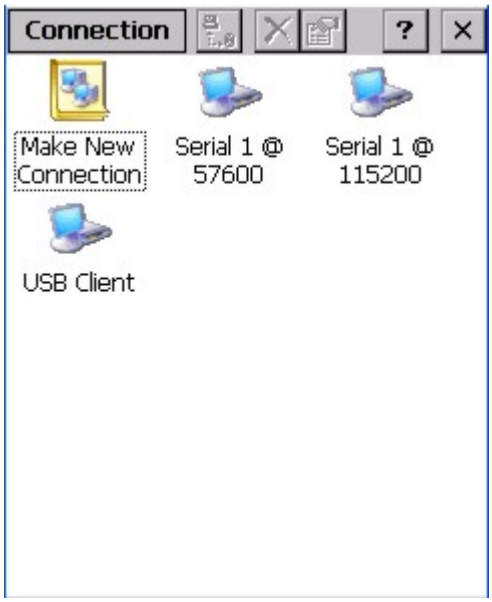
Use this option to set the double-tap sensitivity for stylus taps on the MX9 touchscreen.


Mouse Properties
?
OK
Double-Click
Double-click this grid to set the double-click sensitivity for both the speed and physical distance between
Double-click this icon to test your double-click settings. If this icon doesn't change, adjust your settings using the grid above.

Network and Dialup Options

Start | Settings | Control Panel | Network and Dialup Connections

Set MX9 network driver properties and network access properties. Select a connection to use, or create a new connection.



Create a New Connection

1. On the mobile device, select **Start | Settings | Control Panel | Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the connection you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (My Connection @ 9600, etc.). Tap the **Direct Connection** radio button. Tap the **Next** button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the Port Settings tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off Wait for dial tone, since a direct connection will not have a dial tone. Set the timeout parameter (default is 5 seconds). Tap **OK**.
8. **TCP/IP Settings** should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select **Start | Settings | Control Panel | PC Connection** and tap the **Change Connection…** button.
11. Select the new connection. Tap **OK** twice.
12. Close the Control Panel window.

13. Connect the desktop PC to the mobile device with the appropriate cable.
14. Click the desktop **Connect icon** to test the new connection.

You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

Network Capture

Start | Settings | Control Panel | Network Capture

Note: Verify the date and time before using the logging utilities to ensure meaningful data.

The Network Capture panels provide configuration options for logging utilities.

Two types of logging are configurable:

Netlog is a Windows CE utility that monitors network traffic. Netlog creates a .CAP file that can be read using Microsoft Windows Network Monitor or any compatible tool that supports .CAP files.

NDISLog monitors the the NDIS interface between the Summit radio and the NDIS driver. This utility creates a .TXT log file.

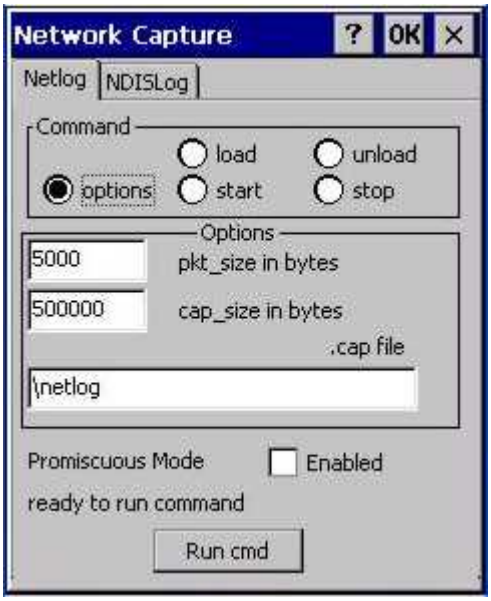
Factory Default Settings

Netlog	
Command	options
pkt_size in bytes	5000
cap_size in bytes	500000
.cap file	\netlog
Promiscuous Mode	Disabled
NDISLog	
Command	stop
file	\ndislog.txt

Netlog

Use this control panel to configure the Netlog utility. By configuring Netlog using the control panel, Netlog remains running across a warmboot. However, please note that:

- Netlog first stores data to a file named netlog0.cap, then netlog1.cap. Any time the current file reaches maximum size, Netlog switches to the other file.
- If the log file is stored in the root directory, any previous data is lost and a new log file started after the warm.boot
- If the log file is stored in \System, all previous data is saved across the warmboot.
- If Netlog is enabled across the warmboot, a series of brief popups may be displayed during the boot cycle. No user inter-action is required.



Command

Command	Function
options	Specifies the option to perform. See the table below for the option parameters and values.
load	Loads and starts Netlog.
start	Starts the Netlog process of logging the network traffic.
stop	Stops Netlog from logging network traffic.
unload	Unloads Netlog.

Options

Options	Function
pkt_size in bytes	Specifies the maximum packet size captured in bytes. This option should only be run after you have called **load** and **stop**. Default is 5000.
cap_siz in bytes	Specifies the maximum size of Netlog0.cap or Netlog1.cap in bytes. This option should only be run after you have called **load** and **stop**. Default is 500,000.
.cap file	Specifies the name of the file to which network traffic information is saved. This option should only be run after you have called **load** and **stop**. Default is \netlog.

Run cmd

Performs the command selected. For example, to run Netlog and modify the packet size do the following:

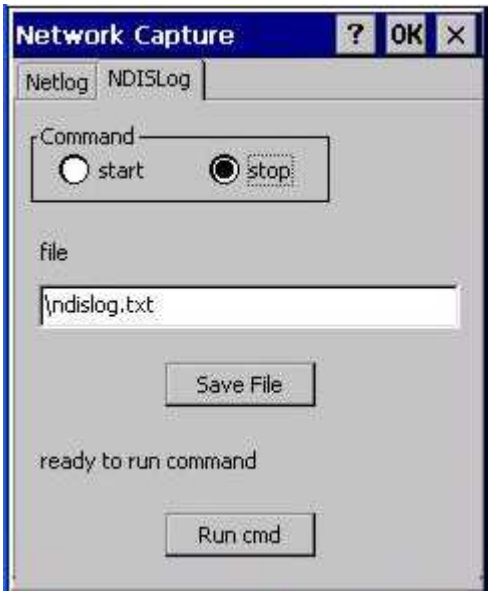
Select **load** from the Commands list and click the **Run cmd** button.

Select **stop** from the Commands list and click the **Run cmd** button.

Select **options** from the Commands list, enter the new packet size in the Options list and click the **Run cmd** button.

NDISlog

NDISLog creates a .TXT file that can be viewed with any text editor program that supports .TXT files.



Command

Command	Function
start	Starts logging the network traffic.
stop	Stops logging network traffic.

file

Specifies the name of the file to which NDISLog information is stored.

Save File

Stores the file name.

Run cmd

Performs the selected start or stop command.

Options

Start | Settings | Control Panel | Options

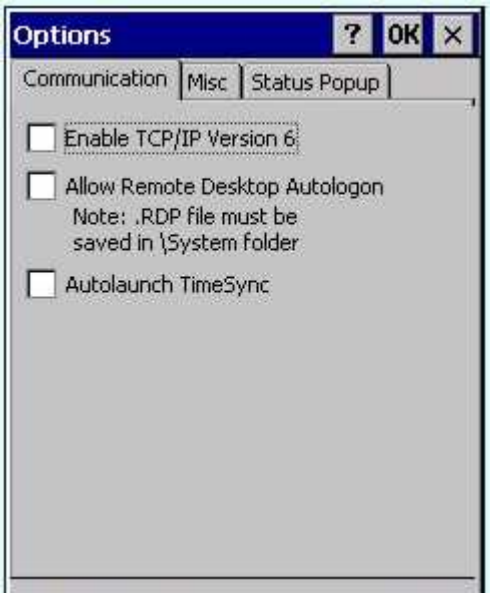
Set options unique to your device, such as keypad backlight, Status Popup taskbar icon display and CapsLock.

It may be necessary to warmboot the MX9 after making desired changes. A pop up window indicates if a warmboot is required.

Note: Contact your LXE representative if there is no icon corresponding to this item in the Control Panel.

Communication

Options on this tab configure communication options for the MX9.



Options / Communication Tab

Enable TCP/IP Version 6

By default, IPv6 is disabled on the LXE device. Check this checkbox to enable IPv6.

Allow Remote Desktop Autologon

By default, Remote Desktop Autologon is disabled. Check this checkbox to enable Remote Desktop Autologon.

Note: The .RDP file must be saved in the \System folder. When prompted, use the Save As button to save the .RDP file is the \System directry. If the .RDP file is saved in the default root folder location, the .RDP file will not persist across a warmboot.

Autolaunch TimeSync

By default, TimeSync does not automatically run on the MX9. To enable TimeSync to run automatically on the MX9, check this checkbox.

Synchronize with a Local Time Server

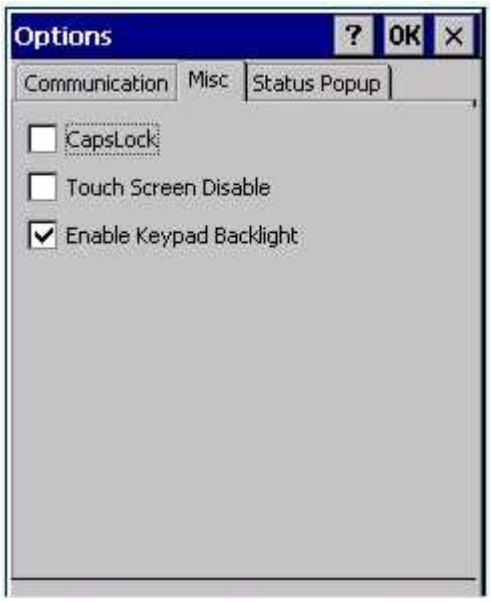
By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

1. Use ActiveSync to copy GrabTime.ini from the My Device | Windows folder on the mobile device to the host PC.
2. Edit the copy of GrabTime.ini on the host PC. Add the local time server's domain name to the beginning of the list of servers. You can optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini file to the My Device | System folder on the mobile device.

The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. System/Grabtime.ini also persists after a coldboot; Windows/Grabtime.ini does not persist.

Misc

Options on this tab configure device specific options. Note that options not available on the MX9 are grayed out.



Options / Misc Tab

CapsLock

By default, CapsLock is disabled after a warmboot. To enable CapsLock after a warmboot, check this checkbox.

Touch Screen Disable

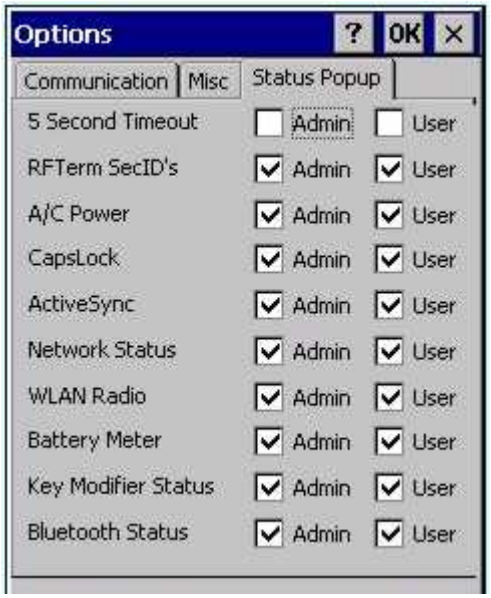
By default, the MX9 touchscreen is enabled. To disable the touchscreen after a warmboot, check this checkbox.

Enable Keypad Backlight

The keypad backlight default setting is to follow the display backlight setting until it is changed by the user.
Uncheck the checkbox to disable the keypad backlight.

Status Popup

Options on this tab configure the Status Popup window. When the Status popup window is displayed, it is placed on top of the window in focus and hides any data beneath it. It is closed by pressing the assigned Status User or Status Admin key sequence.



Options / Status Popup Tab

Using the **KeyPad control panel**, the System Administrator must first assign a **Status User** key sequence for the end-user when they want to toggle the Status Popup Window on or off.

The System Administrator must also assign a **Status Admin** key sequence to perform the same function. Status popup window display options (taskbar icons) are assigned on the Status Popup tab. E.g. AC Power, ActiveSync, WLAN radio, CapsLock, Network status, Bluetooth status, etc.

The default for the User and Admin status popup windows is to show all status information. The 5 second timeout to remove the status popup from the display is disabled by default for the User and Admin status popup windows.

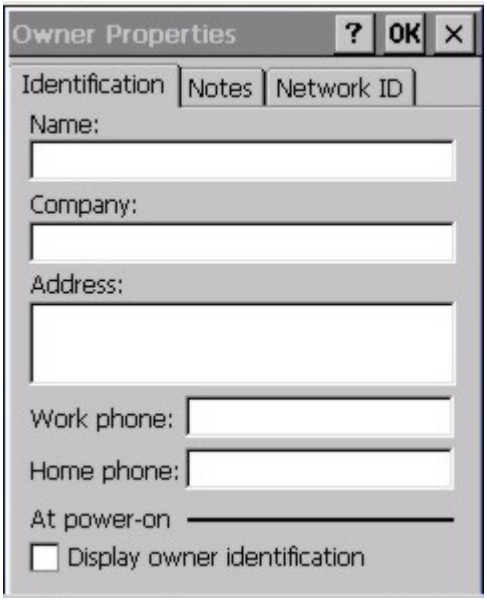
Owner

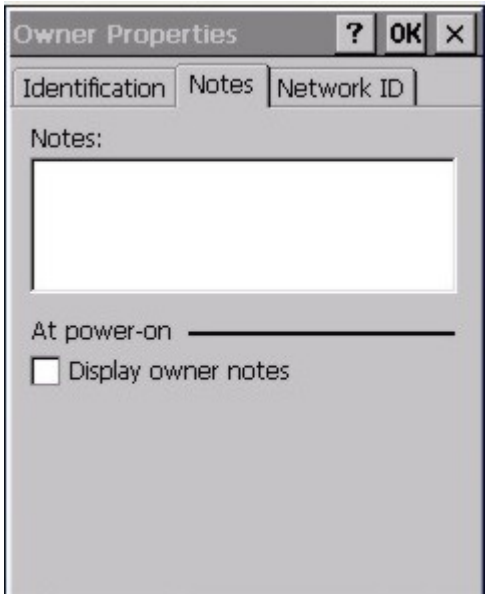
Start | Settings | Control Panel | Owner

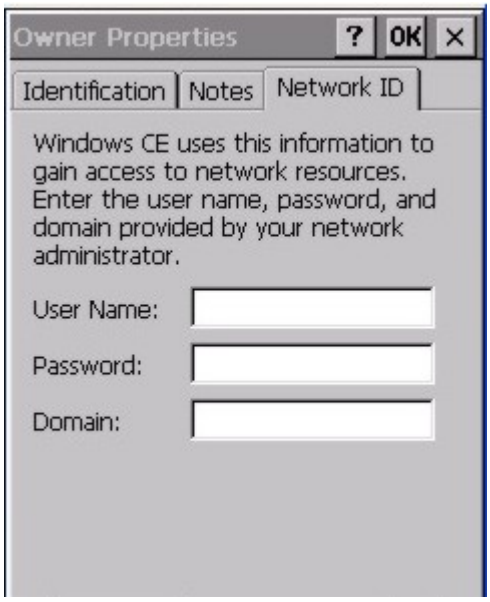
Set the MX9 owner details. The Network ID is used when logging into a remote network.

Factory Default Settings

Identification	
Name	Blank
Company	Blank
Address	Blank
Telephones	Blank
Display owner ID at power-on	Disabled
Notes	
Notes	Blank
Display notes at power-on	Disabled
Network ID	
User Name	Blank
Password	Blank
Domain	Blank







Enter user name, password and domain to be used when logging into network resources.

Password

Start | Settings | Control Panel | Password

Use this panel to set MX9 user access to control panels and power up password properties.

Important: This password must be entered before performing a Load Factory Defaults.

Contact your LXE representative if entering a power-on or screen saver password does not allow you to disable this password protection or perform a Load Factory Defaults.

Factory Default Settings

Password	Blank
Enter password at Power On	Disabled
Enter password at Remote Desktop Screen Saver	Disabled

Enter the password in the Password text box, then press Tab and type the password again to confirm it.

Enable the power-on checkbox and, if desired, the screensaver checkbox.

A changed/saved password is in effect immediately.

Notes:

- The password and password settings are saved during a warm boot and a cold boot.
- The screensaver password affects the Remote Desktop screensaver only.
- After a password is assigned and saved, each time a Settings | Control Panel option is selected, the user will be required to enter the password before the Control Panel will open.
- The screensaver password is the same as the power-on password. They are not set independently.
- A screensaver password cannot be created without first enabling the “Enable password protection at power-on” check-box.
- The screensaver password is not automatically enabled when the “power-on” checkbox is enabled.

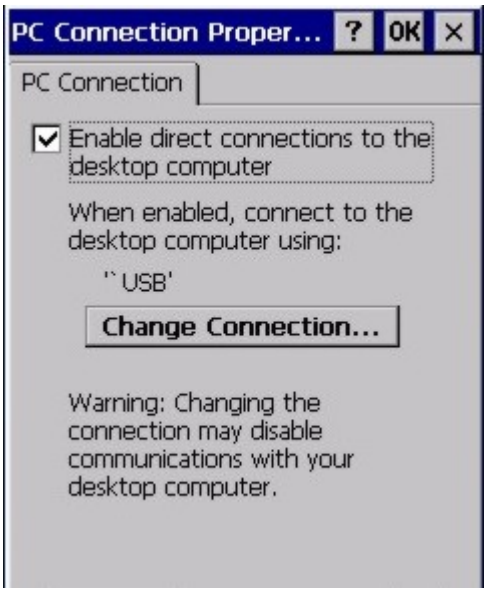
PC Connection

Start | Settings | Control Panel | PC Connection

Use these options to control a cabled connection (USB, serial) between the MX9 and a nearby desktop/laptop computer.

Factory Default Settings

Enable direct connection	Enabled
Connect using	USB Client


PC Connection Proper...
?
OK
PC Connection
Enable direct connections to the desktop computer
When enabled, connect to the desktop computer using:
'' USB'
Change Connection...
Warning: Changing the connection may disable communications with your desktop computer.

Unchecking the **Enable direct connections** checkbox disables ActiveSync on the MX9.

Tap the **Change Connection** button to change the direct connect setting.

Tap the drop down box to view a list of pre-configured connection settings.

Peripherals

Start | Settings | Control Panel | Peripherals

These panels are used to enable and disable the touch screen and scanner window heaters, and they are also used to set the time limit for the flashlight. Using the GPS tab, power to the GPS can be toggled on or off.

Factory Default Settings

Heaters	
Touch screen heater	Enabled
Scanner window heater	Enabled
Flashlight	
Turn flashlight off after	1 minute
GPS	
GPS Power	ON when installed / OFF when not installed

Heaters

Note: Setting has no effect if the heater is not installed.

Click the radio button to enable or disable the heater.

Flashlight

Note: Setting has no effect if the flashlight is not installed.

Select an option to set the timeout for the flashlight. Options are:

- 1 minute
- 2 minutes
- 3 minutes

GPS

GPS presence is displayed on the GPS panel. Power can be toggled on or off only when a GPS is installed. The default setting is Off.

Power

Start | Settings | Control Panel | Power

The MX9 power mode timers are cumulative.

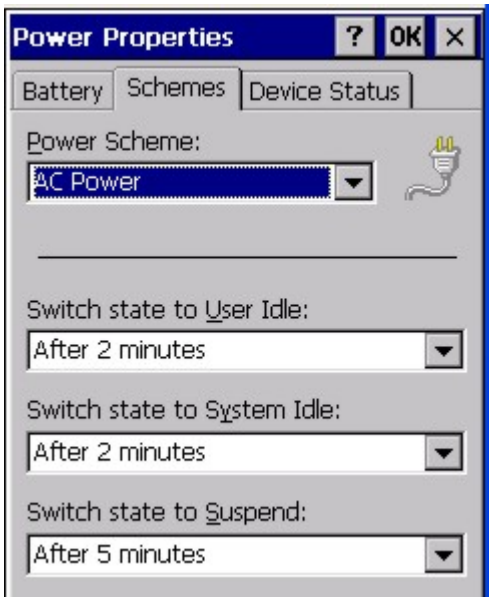
The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired.

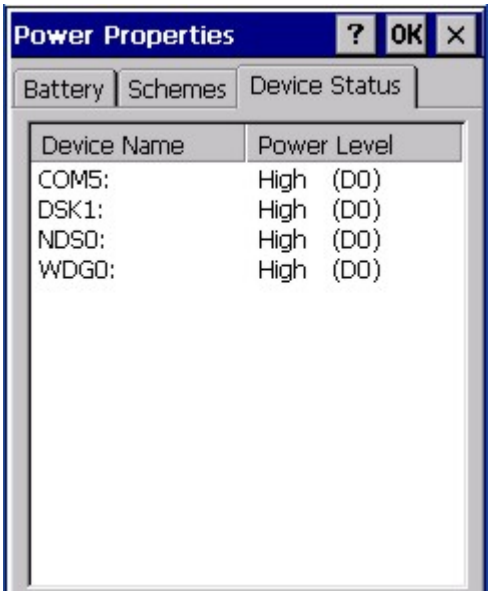
When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

The Display | Backlight setting is synchronized with the User Idle setting in the Schemes tab in the Power control panel.

Factory Default Settings

Battery Tab	
Turbo Mode	Enabled
Schemes Tab	
Battery Power - User Idle Timeout	3 seconds
Battery Power - System Idle Timeout	15 seconds
Battery Power - Suspend Timeout	5 minutes
AC Power - User Idle Timeout	2 minutes
AC Power - System Idle Timeout	2 minutes
AC Power - Suspend Timeout	5 minutes
Device Status Tab	No user interaction





Because of the cumulative effect, and using the Battery Power Scheme Defaults listed above:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15 sec + 3 sec),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.
- If the User Idle timer is set to Never, the power scheme timers never place the device in User Idle, System Idle or Suspend modes.

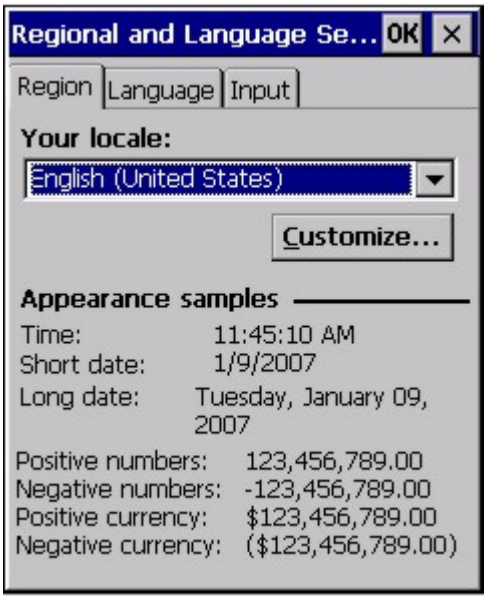
Regional and Language Settings

Start | Settings | Control Panel | Regional Settings

Set the appearance of numbers, currency, time and date based on regional and language settings. Set the MX9 user interface language and the default input language.

Factory Default Settings

Region	
Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US

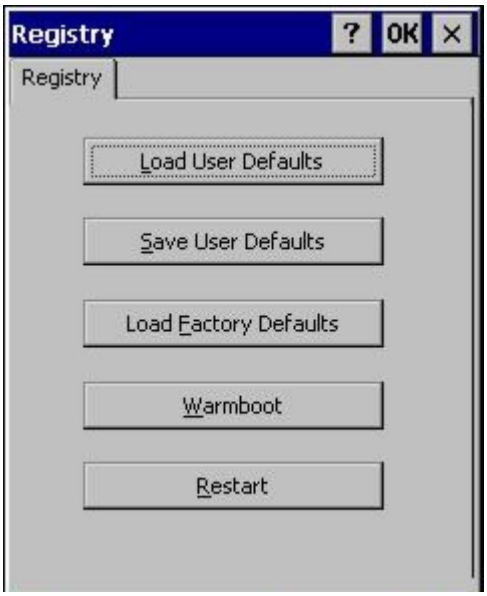


Regional and Language Se...
OK
Region
Language
Input
Default Input Language:
Select the input language to use when you start your device.
English (United States)-US
Installed Input Languages:
Select input languages you plan to use.
English (United States)-US

Registry

Start | Settings | Control Panel | Registry

Choose an MX9 software reload scheme.



Tab	Contents
Load User Defaults	When clicked, a standard load file dialog is opened, to allow the user to pick a Registry Save (.RSG) file. The applet then copies the specified User registry file to the Active registry. The user is asked to verify a reboot, and then the applet does a warmboot to activate the new registry. Load User Defaults takes 20 seconds from SD card, or 10 seconds from internal flash.
Save User Defaults	When clicked, a standard Save File dialog is opened, to allow the user to name the Registry Save (.RSG) file. The applet then copies the Active registry to the specified User registry file. Save User Defaults takes 30 seconds to save to SD card, or 10 seconds to save to internal flash.
Load Factory Defaults	The applet copies the Factory Default registry from the OS to the Active registry (by deleting the current registry). The user is asked to verify a reboot, and then the applet does a restart to activate the factory default registry. If a user password has been set, the applet warns the user that the password will be erased, and asks them to enter it before the reboot is allowed.
Warmboot	When clicked, the OS does a registry flush (Active registry saved to Flash registry hive), and then a warmboot.
Restart	When clicked, the OS does a registry flush, and then a restart.

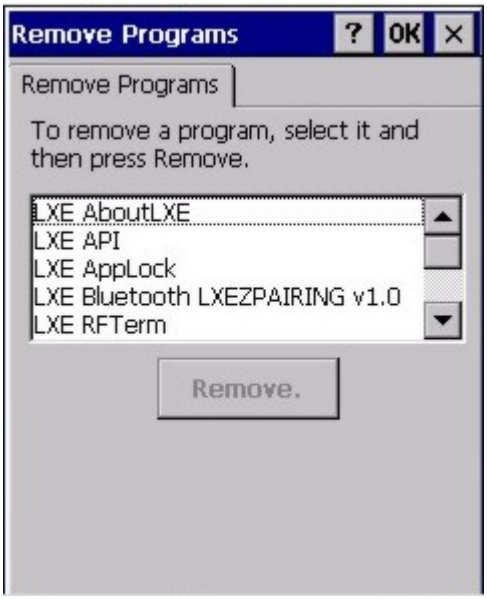
Remove Programs

Start | Settings | Control Panel | Remove Programs

Note: Lists programs installed in RAM that have been marked for removal.

Select a program and tap Remove. Follow the prompts on the screen to uninstall MX9 user-installed only programs. The change takes effect immediately.

Files stored in the **My Documents** folder are not removed using this option.

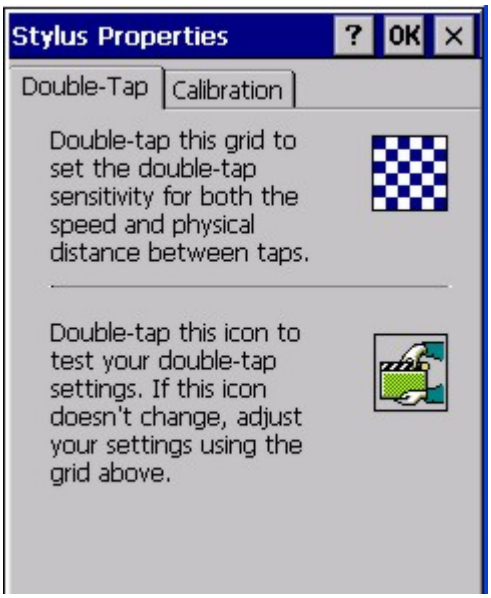


Note: Do not remove LXE-installed programs using this option. Contact your LXE representative for assistance if LXE installed programs must be deleted.

Stylus

Start | Settings | Control Panel | Stylus

Use this control panel option to set stylus double-tap sensitivity properties and calibrate the MX9 touch panel when needed.


Stylus Properties
?
OK
Double-Tap
Calibration
Double-tap this grid to set the double-tap sensitivity for both the speed and physical distance between taps.
Double-tap this icon to test your double-tap settings. If this icon doesn't change, adjust your settings using the grid above.

Double Tap

Follow the instructions on the screen and tap the OK button to save any double tap changes.

Calibration Tab

Calibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

To begin, tap the **Recalibrate** button on the screen with the stylus. Press and hold the stylus on the center of the target as it moves around the screen. Press the Enter key to keep the new calibration setting or press the Esc key to revert to the previous calibration settings.

System

System | Settings | Control Panel | System

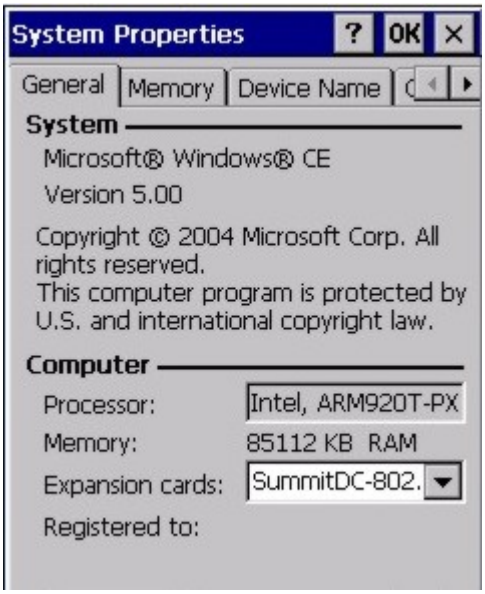
Use these MX9 panels to:

- Review System and mobile device data and revision levels.
- Adjust Storage and Program memory settings.
- Assign a device name and device descriptor.

Factory Default Settings

General	No user interaction
Memory	1/3 storage, 2/3 program memory
Device Name	Unique to equipment type
Device Description	LXE_MX9
Copyrights	No user interaction

General Tab

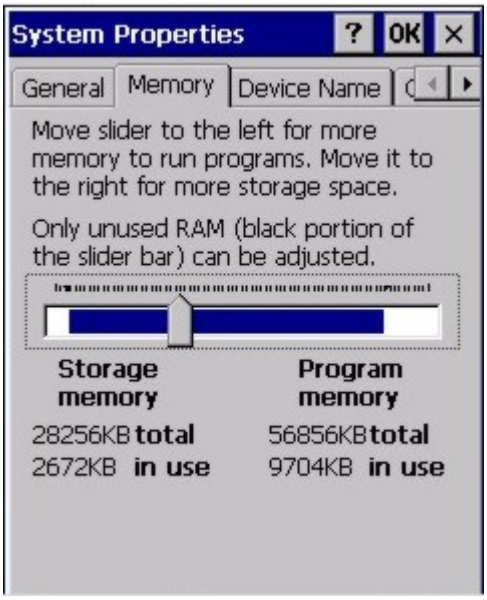


System: This screen is presented for information only. The System parameters cannot be changed by the user.

Computer: The processor type is listed. The type cannot be changed by the user. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

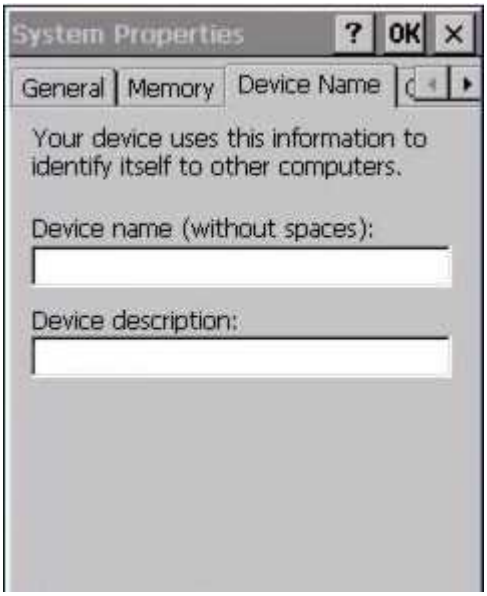
Memory sizes given do not include memory used up by the operating system. For example, a system with 128 MB may only report 99 MB memory, since 29 MB is used by the operating system. This is actual DRAM memory, and does not include internal flash used for storage.

Memory Tab



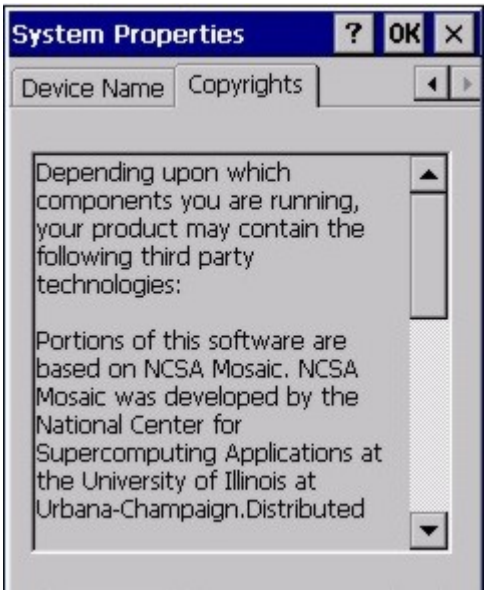
Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the mobile device is running slowly, try increasing the amount of program memory.

Device Name Tab



The device name and description can be changed by the user. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. This information is used to identify the MX9 to other computers and devices.

Copyrights Tab


System Properties
?
OK
Device Name
Copyrights
Depending upon which components you are running, your product may contain the following third party technologies:
Portions of this software are based on NCSA Mosaic. NCSA Mosaic was developed by the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign.Distributed

This screen is presented for information only. The Copyrights information cannot be changed by the user.

Terminal Server Client Licenses

Start | Settings | Control Panel \ Terminal Server Client Licenses

Any licenses stored on the MX9 appear in the drop down list. Select a license and tap the Close button. The license is available for use immediately.

Volume and Sounds

Start | Settings | Control Panel | Volume & Sounds

Note: An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.

Set volume parameters and assign sound WAV files to CE events using these options.

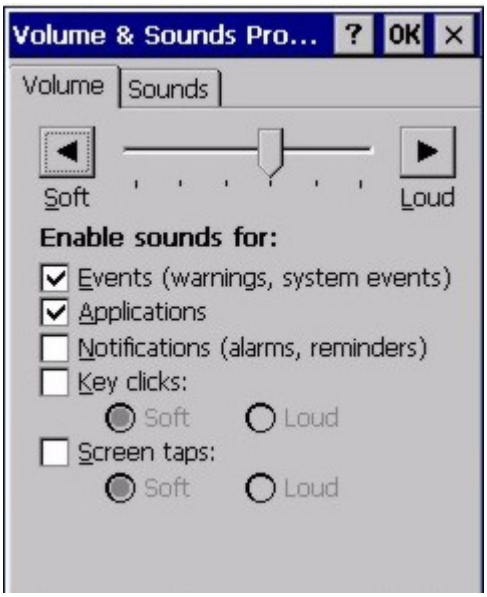
You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

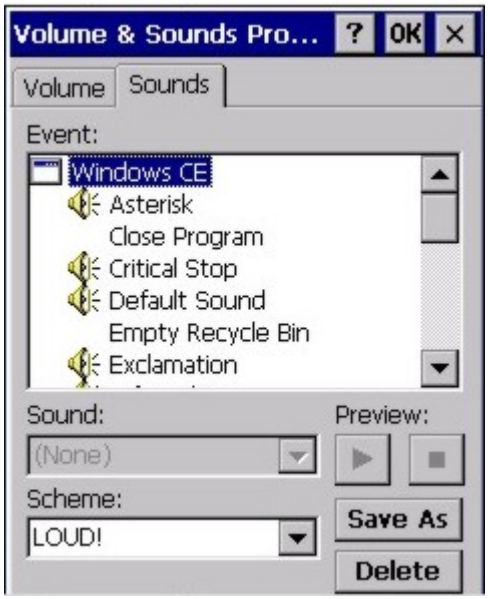
As the volume scrollbar is moved between Loud and Soft, the MX9 emits a tone each time the volume increases or decreases.

Volume must be enabled when you want to adjust volume settings using keypad keys.

Factory Default Settings

Volume	
Events	Enabled
Application	Enabled
Notifications	Disabled
Volume	Middle of Bar
Key click	Disabled
Screen tap	Disabled
Sounds	
Scheme	LOUD!





The volume setting is stored in the registry and is recalled at power on.

Note: Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned barcode data by the barcode processing causes a bad scan beep from the mobile device on the same data.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user's choice.

By default a good scan sound on the MX9 is a single beep, and a bad scan sound is a double beep.

WiFi Control Panel

Start | Settings | Control Panel | WiFi or click the Summit Client Utility icon

Use this option to set parameters and manage profiles for the wireless client pre-loaded on your MX9. See the Summit Client Utility for more information.

WWAN

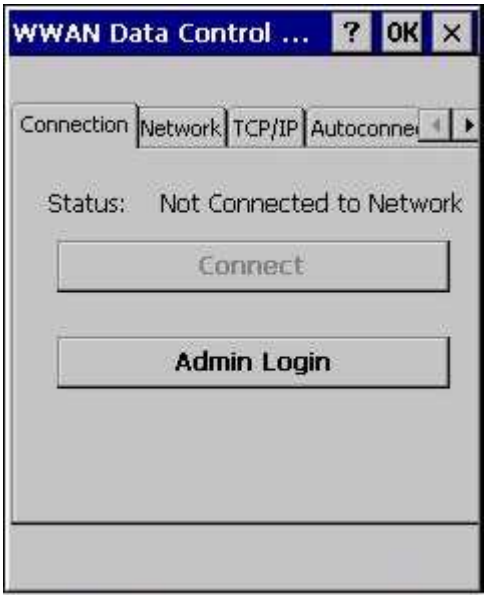
Start | Settings | Control Panel | WWAN

These panels can be used to set the parameters for the Wireless Wide Area Network (WWAN) on the MX9. The WWAN is a form of wireless network that utilizes a cellular network instead of the spread spectrum network most used by Wireless Local Area Networks (WLAN).

Factory Default Settings

Connection	
Status	Not Connected
Network	
Phone, Username, Password, APN	Blank
TCP/IP	
DHCP	Enabled, dimmed
DNS	Enabled, dimmed
Addresses	Pre-populated, dimmed
Autoconnect	
Automatically connect - turned On	Disabled, dimmed
Automatically reconnect	Enabled, dimmed
Admin	
Admin Factory Default Password	LXEWWAN
Enable Radio button	Dimmed

Connection

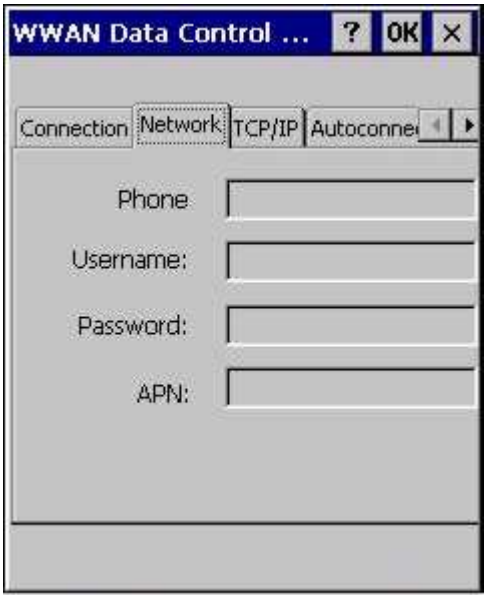


Click the Connect button to begin a connection with a WWAN.

Click the Admin Login button to login.

Enter the password in the popup text box to continue.

Network

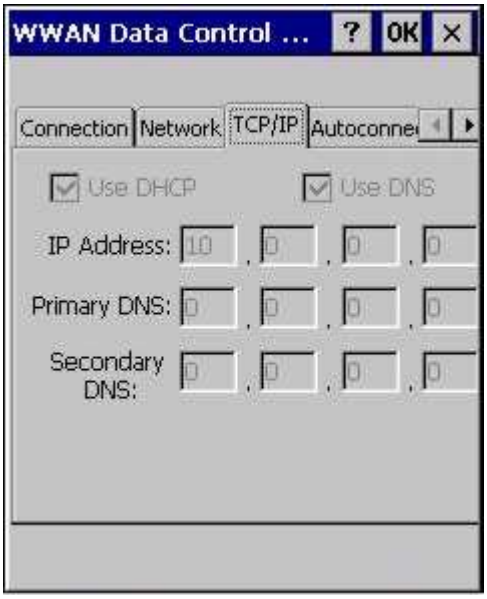


Enter the following information for the MX9:

- Phone (data access number)
- Username

- Password
- APN (Access Point Name)

TCP/IP

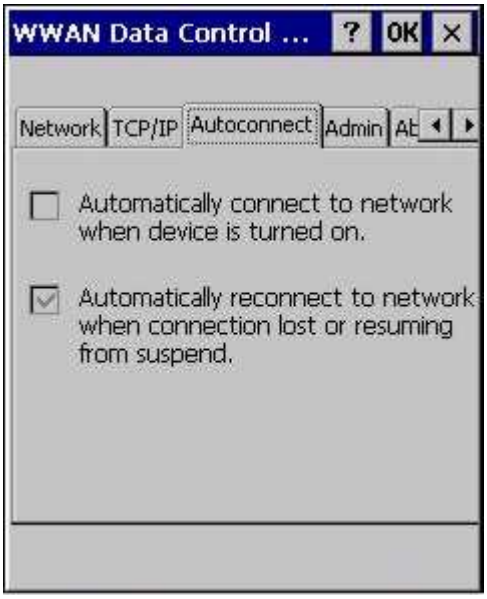


Click the radio button to enable or disable DHCP and/or DNS. When the **Use DHCP** checkbox is enabled, the static IP address is disabled. When the **Use DNS** checkbox is enabled, the DNS address fields are disabled.

If DHCP and DNS are not used, enter the addresses for:

- Static IP Address
- Primary DNS server
- Secondary DNS server

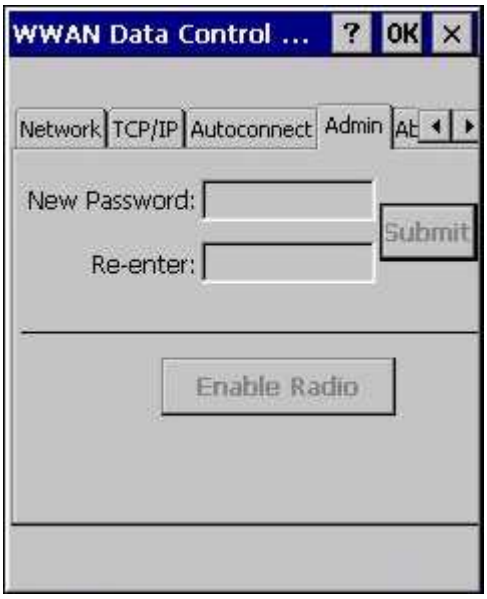
Autoconnect



Automatically connect to network when device is turned on. When this checkbox is enabled (checked) the radio automatically connects to the network when the device is turned on (power button is pressed).

Automatically reconnect to network when connection lost or resuming from suspend. When this checkbox is enabled, the radio automatically attempts to reconnect to the network when it is resumed after being in the suspend state. Automatic reconnection applies whether Autoconnect is on or off.

Admin



Enter a new password, then re-enter the same password. Click Submit to save the new password.

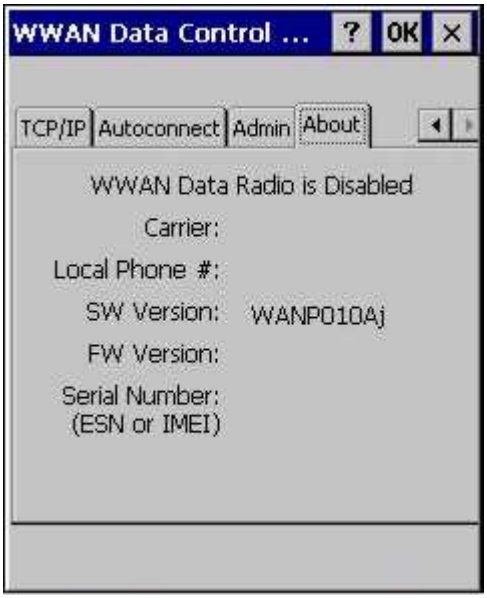
Click the Enable Radio button to turn the radio On or Off. When the radio is Off, the Admin password will need to be entered before the radio can be set to On.

If the radio is currently enabled, the button is labeled Disable. If the radio is currently disabled, the button is labeled Enable.

About

The About tab displays information about the WWAN radio and the current network connection. The About tab displays the SW Version, FW Version and Serial Number of the radio if there is a WAN radio installed in the device. he Local Phone Number shows the subscriber's own number from the SIM card. The current radio enable/disable status is displayed.

The current network Carrier is displayed if the radio is connected. If the radio is not connected to any network, the Carrier entry is blank. In addition to the data shown in the dialog box below, the LXE SW Version is displayed as well. The version matches the corresponding version in the **Start | Settings | Control Panel | About | Versions** dialog box. All fields in the About dialog box are read-only. This information is available to all users without requiring the configuration password.



Some of the information shown on this panel can be edited, after logging in, on previous panels:

- Enable Radio
- Carrier Name
- Local Phone Number

Reflash the MX9

Introduction

Depending on the size of the operating system, the total time required for successful reflashing may require several minutes.

The OS upgrade files are unique to your MX9's physical configuration and date of manufacture. OS upgrade files designed for one device configuration should not be used on a different device configuration.

Preparation

- Contact your LXE representative to get the **OS upgrade files** from LXE.
- Put the **Reflash**[1] files on a desktop/laptop computer with ActiveSync capability.
- Use ActiveSync to back up MX9 user files and store them elsewhere before beginning an upgrade on the MX9.
- Maintain an uninterrupted AC/DC power source to the MX9 throughout this process.
- The MX9 boots from a flash disk.

Procedure

1. Verify a dependable power source is applied to the MX9 and will stay connected during the reflash procedure.
2. Establish an ActiveSync connection between the MX9 and a desktop/laptop computer.
3. Download the reflashing files from the desktop/laptop to the MX9's \System folder.
4. During the file copy process to the MX9 \System folder, when asked “Overwrite ?”, select Yes to All.
5. Disconnect from ActiveSync.
6. Review the files that were downloaded to the \System folder. Some OS update versions include an empty file named REFLASH.TAG. If this file is missing from the download, it must be created and placed in the \System folder. During the reboot process, the device looks for the REFLASH.TAG file in the \System folder. When this file is encountered, the device loads the new bootloader image into the boot flash. The REFLASH.TAG file is deleted and the device is rebooted to begin using the new boot loader.
7. Select **Start | Settings | Control Panel | Registry**. Tap the **Restart** button.
8. It may take several minutes before the device completes the operation.
9. When the OS finishes loading, all software upgrades are complete.
10. Check the OS update version by selecting **Start | Settings | Control Panel | About | Software** tab.

The touch screen may require calibration, however some OS versions save the calibration data, eliminating the need to recalibrate.

[1] Reflashing and flashing are terms used for the process of replacing the existing operating system version with a newer or older operating system version. As the operating system is stored in on-board flash memory, this may be one origin of the term "reflashing".

Reflash Troubleshooting

The powered device won't boot up after reflashing finished.

Send the MX9 to LXE Service and Support to be reflashed.

Warning: Opening the device e.g. exchanging Flash cards, removing endcaps or access panels, etc. could void the user's authority to operate this equipment.

Battery State and OS Upgrade

LXE recommends a fully charged main battery be installed in the MX9 prior to reflashing or upgrading the operating system. A prompt may appear when the battery reaches Critical Low that informs the user there is not enough power in the main battery to perform the update.

The operating system will not be able to execute the OS update when the battery level is too low (25% or less), as there is a high risk that the power remaining in the battery expires when executing the update and the MX9 will be left in an inoperable state.

When main battery power level is too low, connect external power to the MX9 before performing the reflash procedure. Do not disconnect external power before the reflash process is complete.

Troubleshooting

Can’t change the date/time or adjust the volume.	AppLock is installed and may be running in User Mode on the MX9. AppLock user mode restricts access to the control panels.
Touchscreen is not accepting stylus taps or needs recalibration.	Press <Ctrl>+<Esc> to force the Start Menu to appear. Use the tab, backtab and cursor keys to move the cursor from element to element.
MX9 seems to lockup as soon as it is warm booted.	There may be slight delays while the wireless client connects to the network, authorization for voice-enabled applications complete, and Bluetooth relationships establish or re-establish. When the desktop appears or an application begins, the MX9 is ready for use.
New MX9 main batteries don't last more than a few hours.	New batteries must be fully charged prior to first use. Li-Ion batteries (like all batteries) gradually lose their capacity over time (in a linear fashion) and never just stop working. This is important to remember – the MX9 is always ‘on’ even when in the Suspend state and draws a small amount of battery power at all times.
Keep losing ActiveSync connection between my host computer and the MX9.	When the MX9 enters Suspend Mode, all connections are closed to save battery power. When the MX9 wakes up, if ActiveSync connection does not automatically re-establish, disconnect the cable, wait 1-2 seconds and reconnect the cable.

Wireless Network Configuration

The LXE MX9 uses either a Summit 802.11b/g radio or a Summit 802.11a/b/g radio. The radio can be configured for no encryption, WEP encryption or WPA security.

The appropriate wireless utilities for your MX9 configuration have been pre-installed. Your MX9 configuration may consist of one of the following, or several of the following communication devices:

- PAN Radio (Bluetooth)
- WWAN Radio
- WLAN Radio
- GPS Radio

Authentication

Support for a full range of 802.1X (EAP) types, including EAP-TLS, PEAP-MSCHAPv2, PEAP-GTC, LEAP, and EAP-FAST.

Encryption

Support for Static, pre-shared, and dynamic encryption keys 40-bit and 128-bit keys. WEP, WPA (TKIP), and WPA2 (AES) Encryption Methods.

Security Options Supported:

- None
- WEP
- LEAP
- WPA-PSK
- WPA/LEAP
- PEAP-MSCHAP
- PEAP-GTC
- EAP-TLS
- EAP-FAST

Important Notes

Date/Time	It is important that all dates are correct on all computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
	It may be necessary to upgrade radio drivers to in order to use certain Summit Client Utility (SCU) features. Contact your LXE representative for details.
	When using the 802.11a radio, the U-NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U-NII 3 band is allowed, the following channels are supported: 149, 157 and 161. The AP must be configured accordingly.

The Summit radio is either:

- an 802.11a radio: capable of 802.11a, 802.11b and 802.11g data rates.
- an 802.11g radio: capable of 802.11b and 802.11g data rates.

Summit Client Utility

Note: When making changes to profile or global parameters, the device should be warmbooted afterwards.

Access:

Start | Programs | Summit | SCU *or*

SCU Icon on Desktop *or*

Summit Tray Icon (if present) *or*

Wi-FI Icon in the Windows Control Panel (if present)

The Main Tab provides information, admin login and active profile selection.

Profile specific parameters are found on the Profile Tab. The parameters on this tab can be set to unique values for each profile. This tab was labeled Config in early versions of the SCU.

The Status Tab contains information on the current connection.

The Diags Tab provides utilities to troubleshoot the radio.

Global parameters are found on the Global Tab. The values for these parameters apply to all profiles. This tab was labeled Global Settings in early versions of the SCU.

Help

Help is available by clicking the ? icon in the title bar on most SCU screens.

The SCU help may also be accessed by selecting Start | Help and tapping the Summit Client Utility link. The SCU does not have to be accessed to view the help information using this option.

Summit Tray Icon

The Summit tray icon provides access to the SCU and is a visual indicator of radio status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Click the icon to launch the SCU.

Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Wireless Zero Config Utility and the Summit Radio

The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled but the connection is inactive at this time (the device is not connected to a network). The WZC icon may not be visible until control is passed to the WZC utility as described below.

You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. LXE recommends using the Summit Client Utility to connect to your network. The Wireless Zero Configuration Utility cannot control the complete set of security features of the radio.

How To: Use the Wireless Zero Config Utility

1. Select **ThirdPartyConfig** in the Active Profile drop down list as the active profile (see Main Tab).
2. Warmboot the device.

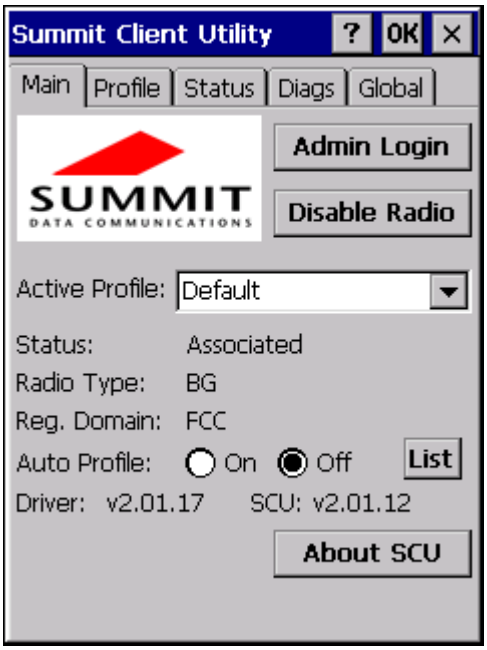
The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, setup radio and security settings.

How to: Switch Control to SCU

1. To switch back to SCU control, select any other profile in the SCU Active Config drop down list, except **Third-PartyConfig**.
2. Warmboot the device.

Radio control is passed to the SCU.

Main Tab



SCU – Main Tab

The Main tab displays information about the radio including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (BG identifies an 802.11b/g radio, ABG identifies an 802.11a/b/g radio)
- Auto Profile option
- Regulatory Domain
- Copyright Info may be accessed by clicking the About SCU button
- Active Profile – Select from the profiles created using the Profile Tab.

Status of the radio (Down, Associated, Authenticated, etc).

The **Disable Radio** button can be used to disable the radio card. Once disabled, the button label changes to **Enable Radio**. By default, the radio is enabled.

The **List** button is used to access the Auto Profile feature.

The **Admin Login** button provides access to editing radio parameters as well as adding, renaming and deleting profiles. Profile and Global parameters may only be edited after entering the Admin Login password. The Active Profile may be changed without logging in. Once logged in, the button label changes to Admin Logout. The admin is also automatically logged out when the SCU is exited.

Admin Login

To login to Admin mode, click the **Admin login** button.

Admin Password Entry

Enter the Admin password and press **OK**. If the password is incorrect, an error message is displayed. The default password is SUMMIT.

Note: The password is case sensitive!

The Admin password can be changed on the Global Tab.

The end user can:

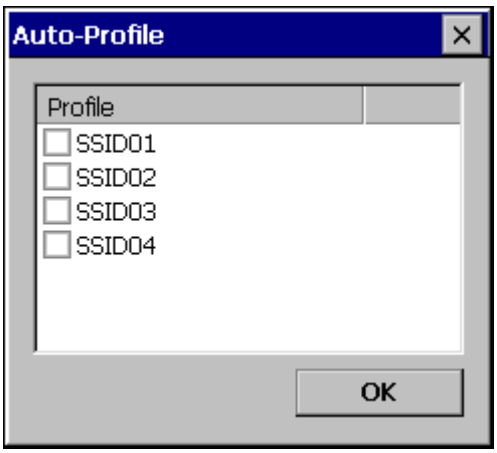
- Turn radio On/Off on the Main Tab
- Select active Profile on the Main Tab
- View the current parameter settings for the profiles on the Profile Tab
- View the global parameter settings on the Global Tab
- View the current connection details on the Status Tab
- View the radio status, software versions and regulatory domain on the Main Tab
- Access additional troubleshooting features on the Diags Tab

After Admin login, the use can also:

- Create, edit, rename and delete profiles on the Profile Tab
- Edit global parameters on the Global Tab

Auto Profile

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, click the List button on the Main tab.



Select Profiles for Auto Profile

The Auto Profile selection screen displays all currently configured profiles. Click on the checkbox for any profiles that are to be included in Auto Profile selection then click **OK** to save.

To enable Auto Profile, click the **On** button on the Main tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

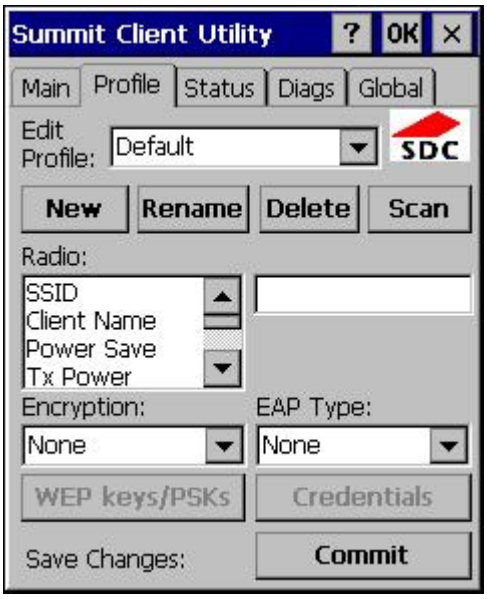
The search continues until:

- the SCU connects to and, if necessary, authenticates with one of the specified profiles or
- until the Off button is clicked to turn off Auto Profile.

Profile Tab

Note: If the Admin password is not entered, the user can view the Profile parameter settings but cannot make any changes. The buttons on this tab are grayed out if the user is not logged in.

The Profile tab was previously labeled Config.



SCU – Profile Tab

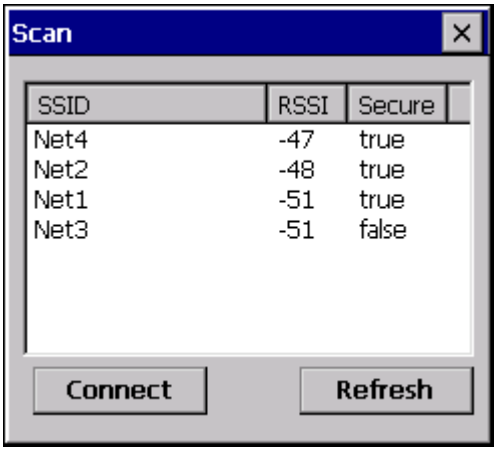
When logged in as an Admin (see Main Tab), use the Profile tab to manage profiles:

- **Rename** – Gives the profile a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.
- **Delete** – Deletes the profile. The current active profile cannot be deleted. In that case, an error message is displayed and the profile is not deleted.
- **New** – Creates a new profile with the default settings (see the list below) and prompts for a name. The name must be unique. If not, an error message is displayed and the profile is not created.
- **Scan** – Scans for and displays a list of available APs. Can be used to create a profile from the APs listed. See Using the Scan Feature
- **Commit** – Ensures that the profile settings made on this screen are saved in the profile.

When not logged in, the parameters can be viewed, but cannot be changed.

Using the Scan Feature

Clicking the **Scan** button opens a pop up window displaying any APs found during the scan.



Scan Results

The scan displays information on the available APs:

- **SSID** – Lists the SSID of the network
- **RSSI** – Displays the Received Signal Strength Indication (RSSI) of the AP.
- **Secure** – Displays True if the data encryption is used by the AP, false is data encryption is not used.

Note: The APs can be sorted by clicking on any of the column headings.

Note: If there is more than one AP with the same SSID, the listing displays the AP with the strongest signal and least security.

If you are logged in as an administrator (see Admin Login), you can use the **Connect** button to create a new profile. The button is grayed out is an administrator is not logged in.

- Highlight the desired network in the listing and click the **Connect** button.
- The new profile is named based on the SSID of the selected AP. If a profile already exists with that name, the new profile name contains an incremental number to avoid duplicate names.
- The SSID parameter is assigned the value of the SSID of the AP. Other profile entries must be completed manually.

Click the **Refresh** button to update the display.

Profile Parameters

IMPORTANT

Remember to click the **Commit** button after making changes to ensure the changes are saved. Newer versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the Profile tab if there are unsaved changes.

If changes are made to the *stored credentials*, click Commit to save those changes before making any additional changes to the Profile parameters.

Profile

A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.

Default:

Default

SSID

A string of up to 32 alphanumeric characters, the Service Set Identifier (SSID) of the WLAN to which the radio connects

Default:

Blank

Client Name

A string of up to 16 characters – Name assigned to the radio and the device using the radio. The client name may be passed to networking radio devices, e.g. Access Points.

Default:

Blank

Power Save

Power save mode.

Options:

CAM (Constantly Awake Mode, power save off)

Maximum (Maximum power saving mode)

Fast (Fast power saving mode)

Default:

Fast

Tx Power

Desired transmit power.

Options:

Maximum (Max power for current regulatory domain)
50, 30, 20, 10, 5 or 1 mW

Default:

Maximum

Bit Rate

Options:

Auto (Rate negotiated automatically with the AP)
1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit

Default:

Auto

Radio Mode

Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio (802.11b/g or 802.11a/b/g) installed in the MX9.

Options:

B rates only (1, 2, 5.5 and 11 Mbps)

BG Rates Full (All B and G rates)

G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps)

BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps)

A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps)

ABG Rates Full (All A rates and all B and G rates with A rates preferred)

BGA Rates Full (All B and G rates and all A rates with B and G rates preferred)

Ad Hoc

Default:

BG Rates Full (for 802.11b/g radio)

BGA Rates Full (for 802.11a/b/g radio)

Note: For the 802.11 b/g radio, some SCU versions may have the default set as BG Optimized rather than BG Rates Full.

It is important this parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only the LXE device may only connect to APs set for G rates and not those set for B and G rates.

The options for this parameter should be set as follows:

Antenna Configuration	Radio Mode
A Main and BG Main	ABG Rates Full BGA Rates Full
A Main and A Aux	A Rates Only
BG Main and BG Aux	B Rates Only G Rates Only BG Rates Full BG Subset

Contact your LXE representative if you have questions about the antenna(s) installed on your device.

Note: Some versions may have the default set as BG Rates Full.

Auth Type

802.11 authentication type used when associating with AP.

Options:

Open

Shared key

LEAP

Default:

Open

Note: Set the Auth Type radio parameter to "Open" for all configurations unless using LEAP (not WPA) and the AP is configured for network EAP only. In this case, set the Auth Type radio parameter to "LEAP".

EAP Type

Extensible Authentication Protocol (EAP) type used for 802.1x authentication to AP.

Options:

None

LEAP

EAP-FAST

PEAP-MSCHAP

PEAP-GTC

EAP-TLS

Default:

None

Note: The EAP type chosen determines if the Credentials button is active. Available entries on the Credentials pop up window vary by EAP type chosen.

Encryption

Type of encryption used to protect transmitted data. This parameter was labeled as Security in some versions of the SCU.

Options:

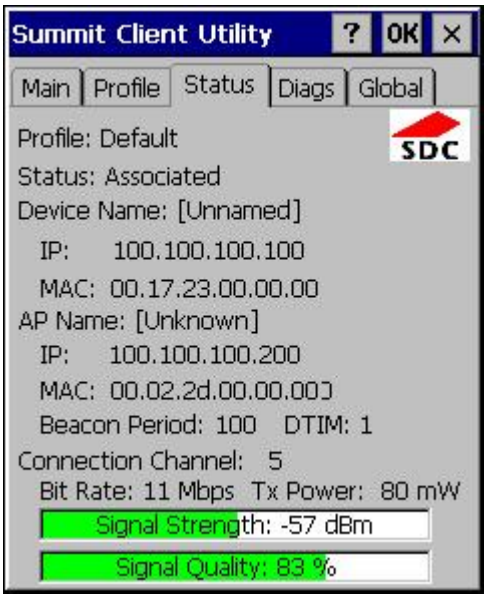
None
Manual WEP
Auto WEP
WPA PSK
WPA TKIP
WPA2 PSK
WPA2 AES
CCKM TKIP
CKIP Manual
CKIP Auto

Default:

None

Note: The Encryption type chosen determines if the WEP/PSK Keys button is active. Available entries on the pop up window vary by encryption type chosen.

Status Tab



SCU – Status Tab

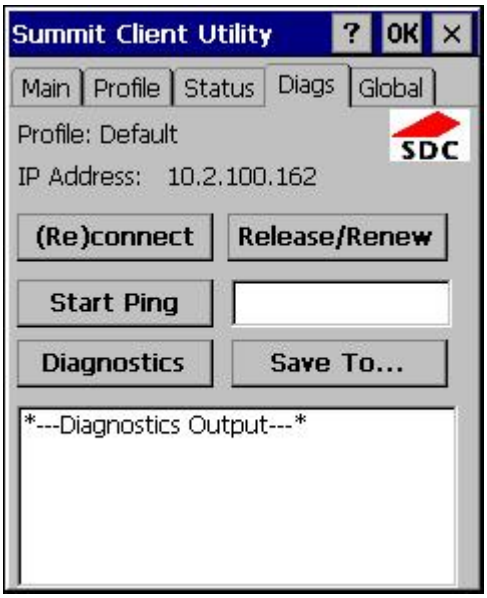
This screen provides information on the radio:

- The profile being used
- The status of the radio card (down, associated, authenticated, etc.)
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic
- Bit rate in Mbit.
- Current transmit power in mW
- Beacon period – the time between AP beacons in kilomircoseconds. (one kilomicrosecond = 1,024 microseconds)
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab



SCU – Diags Tab

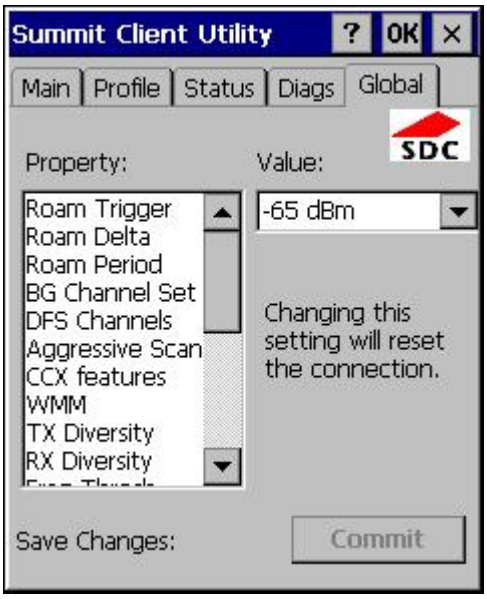
The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

- **(Re)connect** – Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.
- **Release/Renew** – Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.
- **Start Ping** – Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is clicked, the ping begins and the button label changes to **Stop Ping**. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.
- **Diagnostics** – Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.
- **Save To…** – Use this save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global Tab

Note: The Global tab was previously labeled Global Settings.

The parameters on the global settings tab can be changed when an Admin is logged on (see Admin Login). Without the admin login, the current values for the parameters can be viewed, but they cannot be edited.



SCU – Global Tab

Global Parameters

IMPORTANT

Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt it made to close or browse away from the Global tab if there are unsaved changes.

If changes are made to the *stored credentials*, click Commit to save those changes before making any additional changes to the Global parameters.

Note: Custom parameter options: Some parameters contain an option for custom. The parameter's value is displayed as "Custom" when the operating system registry has been used to set the parameter to a value not available from the Global settings parameter options. Selecting Custom for a parameter has no effect as the parameter value returns to the previously selected value when you press Commit.

Roam Trigger

If signal strength is less than this trigger value, the radio looks for a different AP with a stronger signal.

Options:

-50, -55, -60, -65, -70, -75, -80, -85, -90 dBm

Custom (see Note)

Default:

-65 dBm

Note: Custom parameter options: Some parameters contain an option for custom. The parameter's value is displayed as "Custom" when the operating system registry has been used to set the parameter to a value not available from the Global settings parameter options. Selecting Custom for a parameter has no effect as the parameter value returns to the previously selected value when you press Commit.

Roam Delta

Amount by which the new AP's signal strength must exceed the current AP's signal strength before roaming is attempted.

Options:

5, 10, 15, 20, 25, 30, 35 dBm

Custom (see Note above)

Default:

10 dBm (for 802.11b/g radio)

5 dBm (for 802.11a/b/g radio)

Note: Custom parameter options: Some parameters contain an option for custom. The parameter's value is displayed as "Custom" when the operating system registry has been used to set the parameter to a value not available from the Global settings parameter options. Selecting Custom for a parameter has no effect as the parameter value returns to the previously selected value when you press Commit.

Roam Period

The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made.

Options:

5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 sec

Custom (see Note above)

Default:

10 seconds (for 802.11b/g radio)

5 seconds (for 802.11a/b/g radio)

Note: Custom parameter options: Some parameters contain an option for custom. The parameter's value is displayed as "Custom" when the operating system registry has been used to set the parameter to a value not available from the Global settings parameter options. Selecting Custom for a parameter has no effect as the parameter value returns to the previously selected value when you press Commit.

BG Channel Set

Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search roaming time may be reduced over scanning all channels.

Options:

Full (all channels)

1, 6, 11 (the most commonly used channels)

1, 7, 13 (For ETSI and TELEC radios only)

Custom (see Note above)

Default:

Full

Note: Custom parameter options: Some parameters contain an option for custom. The parameter's value is displayed as "Custom" when the operating system registry has been used to set the parameter to a value not available from the Global settings parameter options. Selecting Custom for a parameter has no effect as the parameter value returns to the previously selected value when you press Commit.

DFS Channels

Note: Not currently supported.

Support for 5GHz 802.11a channels where support for DFS is required.

Options:

On, Off

Default:

Off

Aggressive Scan

When set to On and the current connection to an AP becomes weak, the radio scans for available APs more aggressively. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference because of overlapping APs on the same channel.

Options:

On, Off

Default:

On

CCX Features

Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features.

Options:

Full or On (Use Cisco Information Element and CCX version number, support all CCX features)

Optimized (Use Cisco Information Element and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management)

Off (Do not use Cisco Information Element and CCX version)

Default:

Off (for 802.11b/g radio)

Optimized (for 802.11a/b/g radio)

WMM

Use of Wi-Fi Multimedia extensions.

Options:

On, Off

Default:

Off

Auth Server

Specifies the type of authentication server.

Options:

Type 1 (ACS server)
Type 2 (non-ACS server)

Default:

Type 1

TX Diversity

How to handle antenna diversity when transmitting packets to AP.

Options:

Main only (Main antenna only)
Aux only (Aux antenna only)
On (Use diversity)

Default:

On (802.11b/g radio)
Main Only (802.11a/b/g radio)
The value for this parameter should be set as follows:

Antenna Configuration	TX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On
BG Main and BG Aux	On

RX Diversity

How to handle antenna diversity when receiving packets from AP.

Options:

Main Only (use main antenna only)

Aux Only (use aux. antenna only)

On-start on Main (On startup use main antenna)

On-start on Aux (On startup use aux antenna)

Default:

On-start on Main (802.11b/g radio)

Main Only (802.11a/b/g radio)

The value for this parameter should be set as follows:

Antenna Configuration	RX Diversity
A Main and BG Main	Main Only
A Main and A Aux	On-start on Main
BG Main and BG Aux	On-start on Main

Frag Thresh

If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

Options:

256 to 2346

Default:

2346

RTS Thresh

If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point.

Options:

0 to 2347

Default:

2347

LED

The LED on the radio card is not visible to the user when the radio card is installed in a sealed MX9.

Options:

On, Off

Default:

Off

Tray Icon

Determines if the Summit icon is displayed in the system tray.

Options:

On, Off

Default:

On

Hide Password

If On, the Summit Client Utility masks passwords as they are typed and when they are viewed.

Options:

On, Off

Default:

On (see note below)

Note: The default value depends on the SCU revision, some have the default as Off.

Admin Password

A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry text box. The password is Case Sensitive.

Default:

SUMMIT

Note: Password is case sensitive.

Auth Timeout

Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail.

If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed.

If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials.

Options:

An integer from 3 to 60

Default:

8

Certs Path

A valid directory path, of up to 64 characters, where Root CA certificates for EAP authentication (PEAP/MSCHAP, PEAP/GTC, EAP-TLS) and manual PACs for EAP-TLS are stored.

The Windows certificate store can also be used to store Root CA certificates. User certificates (EAP-TLS) must be stored in the Windows certificate store.

LXE suggests ensuring the directory path currently exists before assigning the path in this parameter. For example, if the certificate is stored in My Computer/System/mycertificate.cer, enter System in the Certs Path text box as the directory path.

Default:

System

Ping Payload

Maximum amount of data to be transmitted on a ping.

Options:

32, 64, 128, 256, 512, 1024 bytes

Default:

32

Ping Timeout ms

The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout.

Options:

0 to 30,000 ms

Default:

5000

Ping Delay ms

The amount of time, specified in milliseconds, between each ping.

Options:

0 to 30,000 ms

Default:

1000

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers two choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The Username and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

How to: Use Stored Credentials

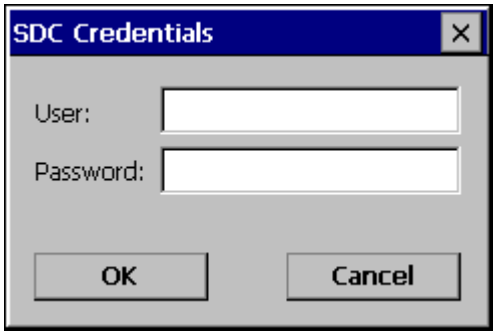
1. After completing the other entries in the profile, click on the **Credentials** button.
2. Enter the Username and Password on the Credentials screen and click **the OK** button.
3. Click the **Commit** button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
6. For EAP-TLS, also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password..
11. Click the **OK** button then the **Commit** button.
12. If changes are made to the stored credentials, click **Commit** to save those changes before making any additional changes to the profile or global parameters.
13. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

Note: See Configuring the Profile for more details.

Note: If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed and the user is not prompted to enter valid credentials.

How to: Use Sign On Screen

1. After completing the other entries in the profile, click on the **Credentials** button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or LEAP/WPA.
2. For PEAP-MSCHAP, PEAP-GTC and EAP-TLS import the CA certificate into the Windows certificate store.
3. For EAP-TLS, also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the **Validate serve**r and **Use MS store** checkboxes are checked.
5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
7. Click the **OK** button then the **Commit** button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the Username and Password. Click the **OK** button.



Sign-On Screen

10. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status Tab indicates the device is Authenticated and the method used.
11. The sign-on screen is displayed after a reboot.

Note: See Configuring the Profile for more details.

If a user enters invalid credentials and clicks **OK**, the device associates but does not authenticate. The user is again prompted to enter credentials.

If the user clicks the **Cancel** button, the device does not associate. The user is not prompted again for credentials until

- the device is rebooted,
- the radio is disabled then enabled,
- the **Reconnect** button on the Diags Tab is clicked or
- the profile is modified and the **Commit** button is clicked.

Windows Certificate Store vs. Certs Path

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, see Generating a User Certificate.
- To import the user certificate into the Windows certificate store, see Installing a User Certificate.
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS. PEAP/GTC. PEAP/MSCHAP. EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

How To: Use the Certs Path

1. See Generating a Root CA Certificate and follow the instructions to download the Root Certifcate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Please note the location chosen for certificate storage should persist after warmboot.
3. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. Enter the certificate name in the CA Cert textbox.
5. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use Windows Certificate Store

1. See Generating a Root CA Certificate and follow the instructions to download the Root Certifcate to a PC.
2. To import the certificate into the Windows store, See Installing a Root CA Certificate.
3. When completing the Credentials screen for the desired authentication, be sure to check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. The default is to use all certificates in the store. If this is OK, skip to the last step.
5. Otherwise, to select a specific certificate click on the **Browse (...)** button.

Choose Certificate

6. Uncheck the **Use full trusted store** checkbox.
7. Select the desired certificate and click the **Select** button to return the selected certificate to the CA Cert textbox.
8. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

Configuring the Profile

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

- On the Main Tab, click the Admin Login button and enter the password.
- LXE recommends editing the default profile with the parameters for your network. Select the Default profile from the pull down menu.
- Make any desired parameter changes as described in the applicable following section determined by network security type and click the **Commit** button to save the changes.

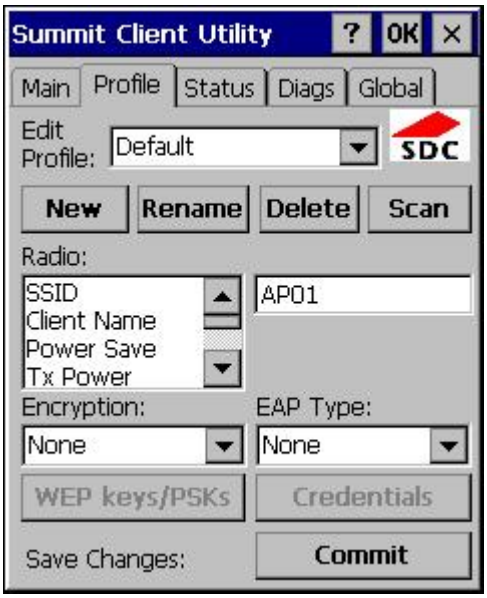
IMPORTANT – Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the *stored credentials*, click Commit to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **None**
- Set **Auth Type** to **Open**



No Security Profile Configuration

Once configured, click the **Commit** button. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

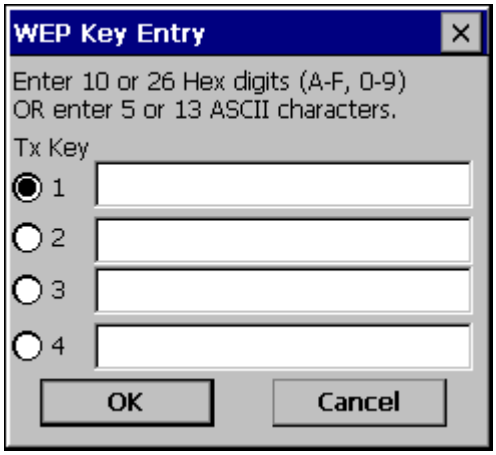
WEP

To connect using WEP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **Manual WEP**
- Set **Auth Type** to **Open**

WEP Profile Configuration

Click the **WEP keys/PSKs** button.



WEP Keys

Valid keys are 10 (for 40-bit encryption) or 26 (for 128-bit encryption) hexadecimal characters. Enter the key(s) and click **OK**.

Once configured, click the Commit button. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP

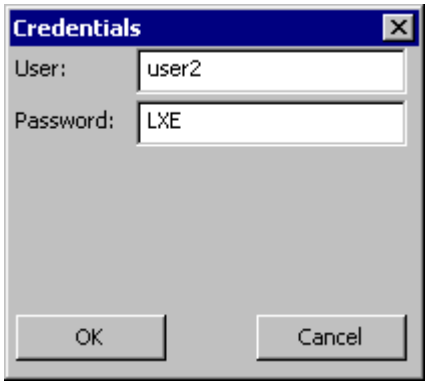
To use LEAP (without WPA), make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **Auto WEP**
- Set **Auth Type** as follows:
  - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
  - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.

LEAP Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



WPA/LEAP Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

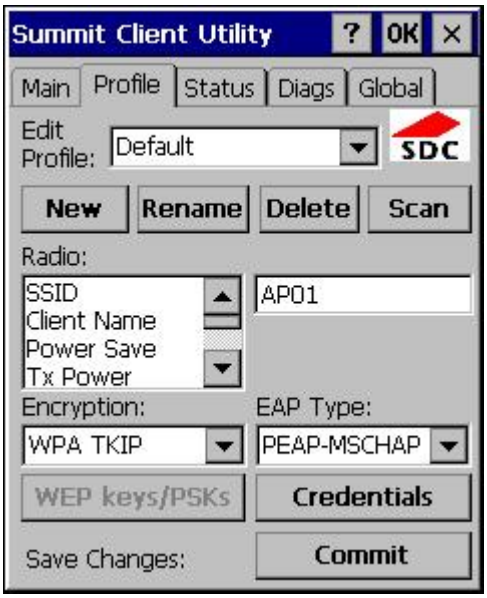
Enter the password.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main Tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

To use PEAP/MSCHAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-MSCHAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**



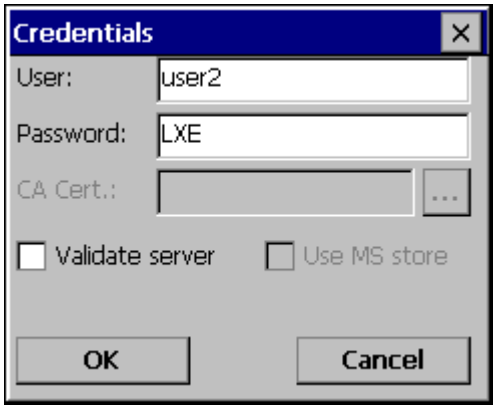
PEAP/MSCHAP Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



PEAP/MSCHAP Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

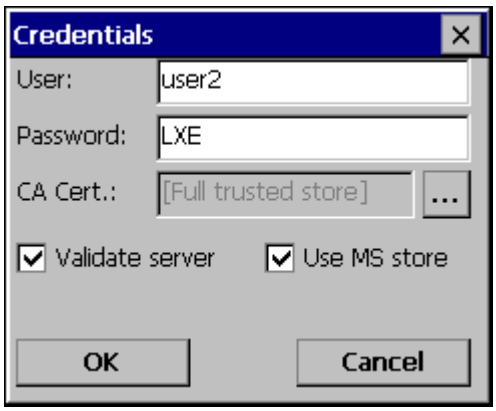
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active profile is selected on the Main Tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



PEAP/MSCHAP Certificate Filename

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click Select. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store** box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

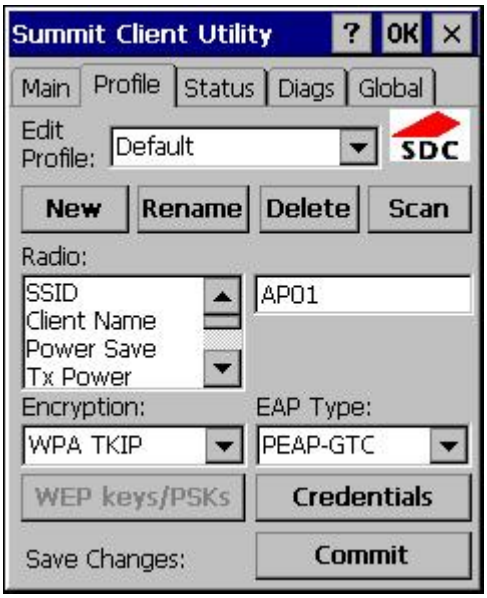
The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Note: The date must be properly set on the device to authenticate a certificate.

PEAP/GTC

To use PEAP/GTC, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-GTC**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**



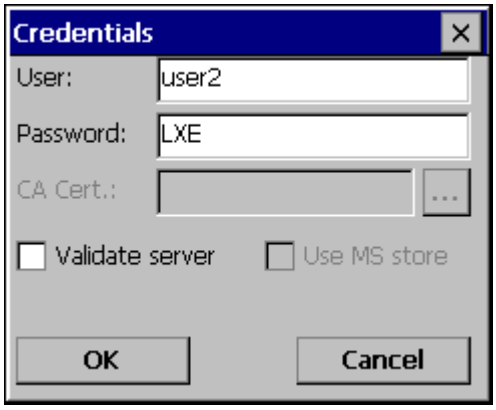
PEAP/GTC Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.

Enter these items as directed below.



PEAP/GTC Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

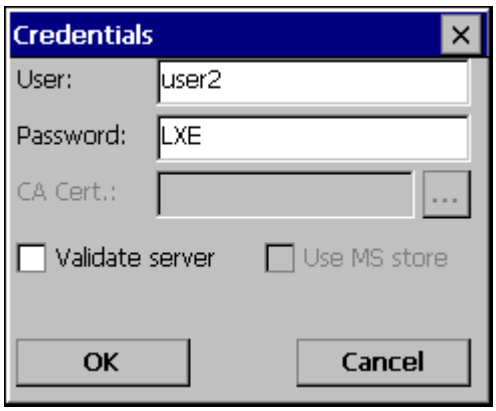
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main Tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



PEAP/GTC Certificate Filename

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store box** unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

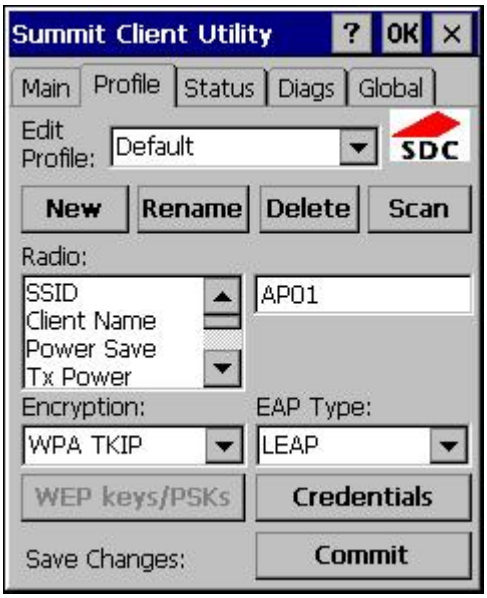
The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Note: The date must be properly set on the device to authenticate a certificate.

WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

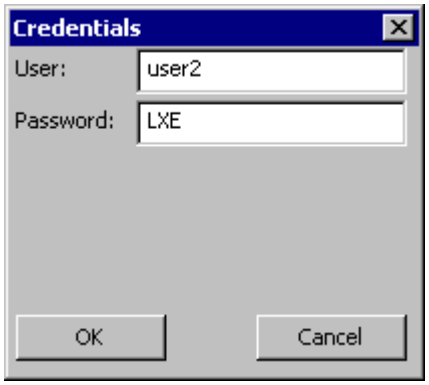
- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** as follows:
  - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
  - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.



WPA/LEAP Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



WPA/LEAP Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

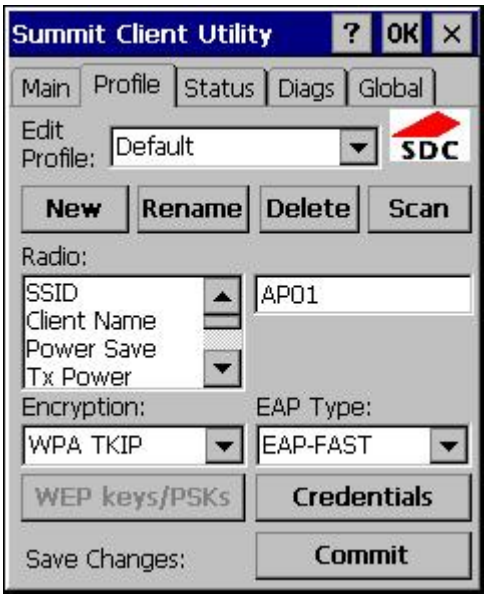
Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main Tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

EAP-FAST

To use EAP-FAST, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-FAST**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the MX9.



EAP-FAST Profile Configuration

For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the MX9. The same username/password must be used to authenticate each time. See the note below for more details.

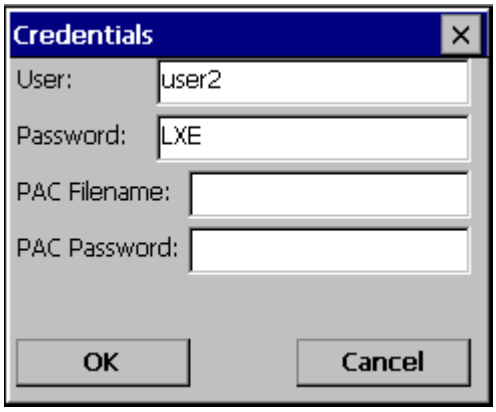
For manual PAC provisioning, the PAC filename and Password must be entered.

See Sign-On vs. Stored Credentials for information on entering credentials.

The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).

Click on the **Credentials** button.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the Username and Password when connecting to the network.



EAP-FAST Credentials

To use Sign-On credentials:

- Do not enter a User and Password as the user will be prompted for the Username and Password when connecting to the network.

To use Stored Credentials:

- Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
- Enter the password.

To use Automatic PAC Provisioning:

- No additional entries are required.

To use manual PAC Provisioning:

- Enter the PAC Filename and PAC Password.
- The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.

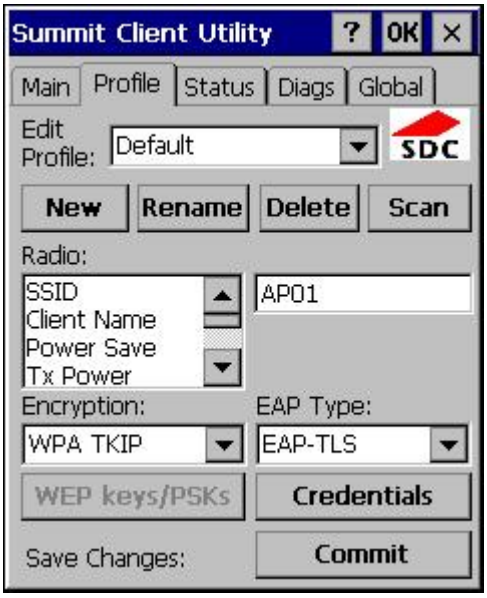
Tap **OK** then tap **Commit**. Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

EAP-TLS

To use EAP-TLS, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-TLS**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**



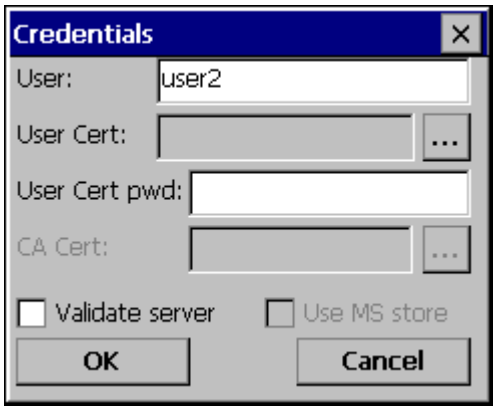
EAP-TLS Profile Configuration

See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



EAP-TLS Credentials

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Leave the certificate file name entries blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main tab.

Once successfully authenticated, import the user certificate into the Windows certificate store.

Return to the Credentials screen.

Use the **Browse** button to locate the User Cert from the certificate store. Highlight the desired certificate and press the **Select** button. The name of the certificate is displayed in the User Cert box.

Enter the password for the user certificate in the User Cert pwd box.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Check the **Validate server** checkbox.

EAP-TLS Credentials

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The MX9 should be authenticating the server certificate and using EAP-TLS for the user authentication.

See Certificates for information on generating a Root CA certificate or a User certificate.

Note: The date must be properly set on the device to authenticate a certificate.

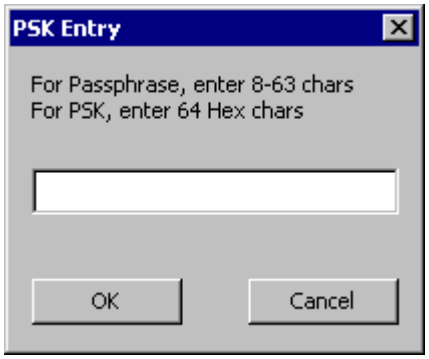
WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WPA PSK**
- Set **Auth Type** to **Open**

WPA/PSK Profile Configuration

Click the **WEP keys/PSKs** button.



PSK Entry

This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click **OK**.

Once configured, click the **Commit** button. Ensure the correct Active Profile is selected on the Main Tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

Certificates

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

See Generating a Root CA Certificate

See Installing a Root CA Certificate

User Certificates are necessary for EAP-TLS

See Generating a User Certificate

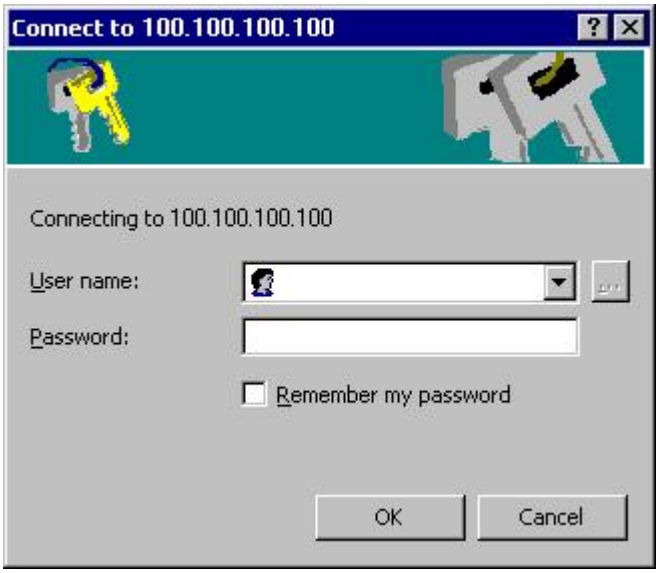
See Installing a User Certificate

Generating a Root CA Certificate

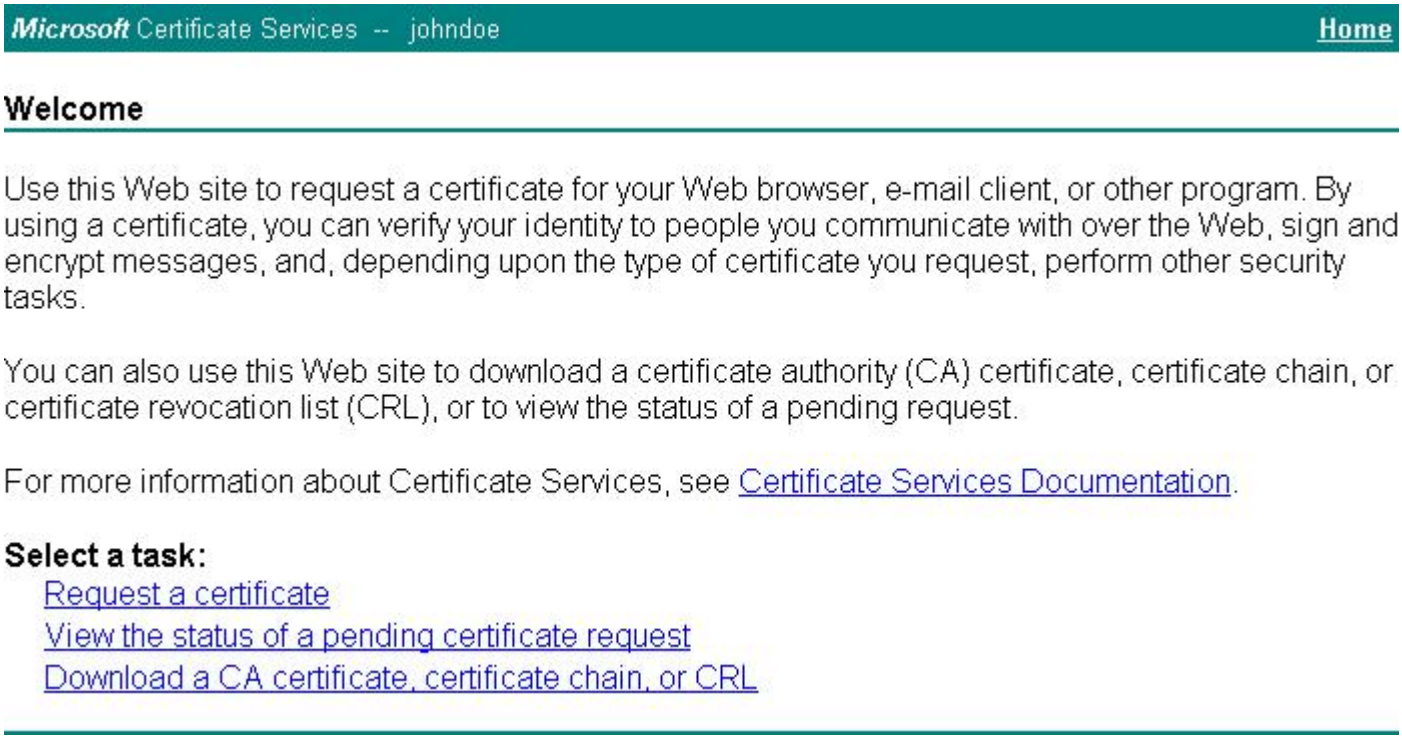
The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the Certificate Authority. To request the root CA certificate, open a browser to

http://<CA IP address>/certsrv.

Sign into the CA with any valid username and password.



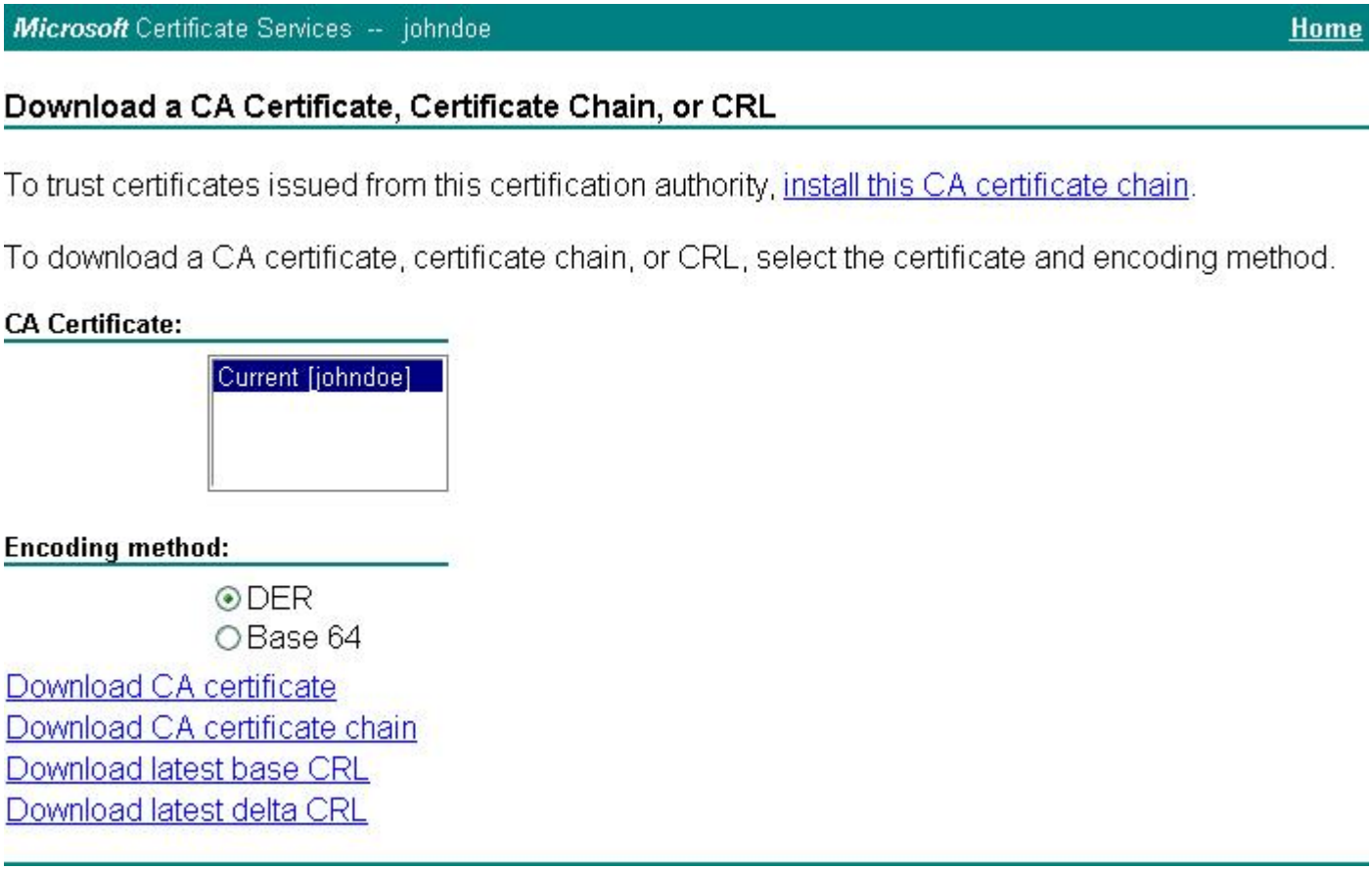
Logon to Certificate Authority


Microsoft Certificate Services -- johndoe
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Certificate Services Welcome Screen

Click the **Download a CA certificate, certificate chain or CRL** link.

Make sure the correct root CA certificate is selected in the list box.


Microsoft Certificate Services -- johndoe
Home
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority, install this CA certificate chain.
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
CA Certificate:
Current [johndoe]
Encoding method:
DER
Base 64
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Download CA Certificate Screen

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.

File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 1.10 KB
From: 100.100.100.100
Open
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Download CA Certificate Screen

Click the **Save** button and save the certificate. Make sure to keep track of the name and location of the certificate.

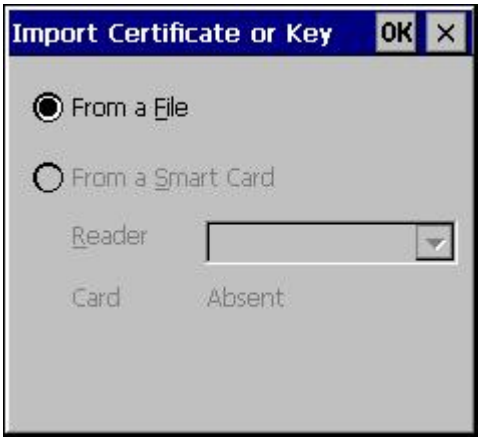
Installing a Root CA Certificate

Note: This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the \System folder or other path specified in the Summit Certs global parameter.

Copy the certificate file to the MX9. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Certificates

Tap the **Import** button.



Import Certificate

Make sure **From a File** is selected and tap **OK**.

Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.

Root Certificate Store
Do you want to ADD the following certificate to the Root Store?
Subject : doe, SUPPORT, LOCAL
Issuer : Self Issued
Time Validity : Thursday, July 01, 2004 through Tuesday, July 01, 2014
Serial Number : 12345678 90ABCDEF 12345678 90ABCDEF
Yes
No

Certificate Import Confirmation

Tap **Yes** to import the certificate.

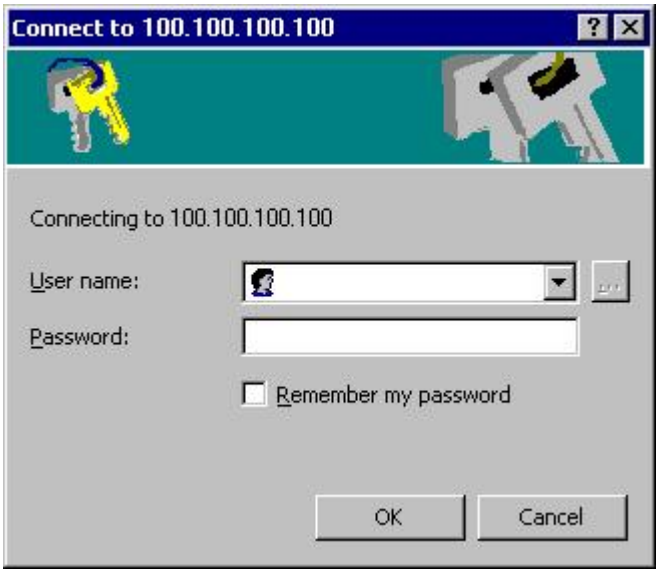
Once the certificate is installed, return to the proper authentication section, earlier in this manual.

Generating a User Certificate

The easiest way to get the user certificate is to use a browser on a PC to navigate to the Certificate Authority. To request the user certificate, open a browser to

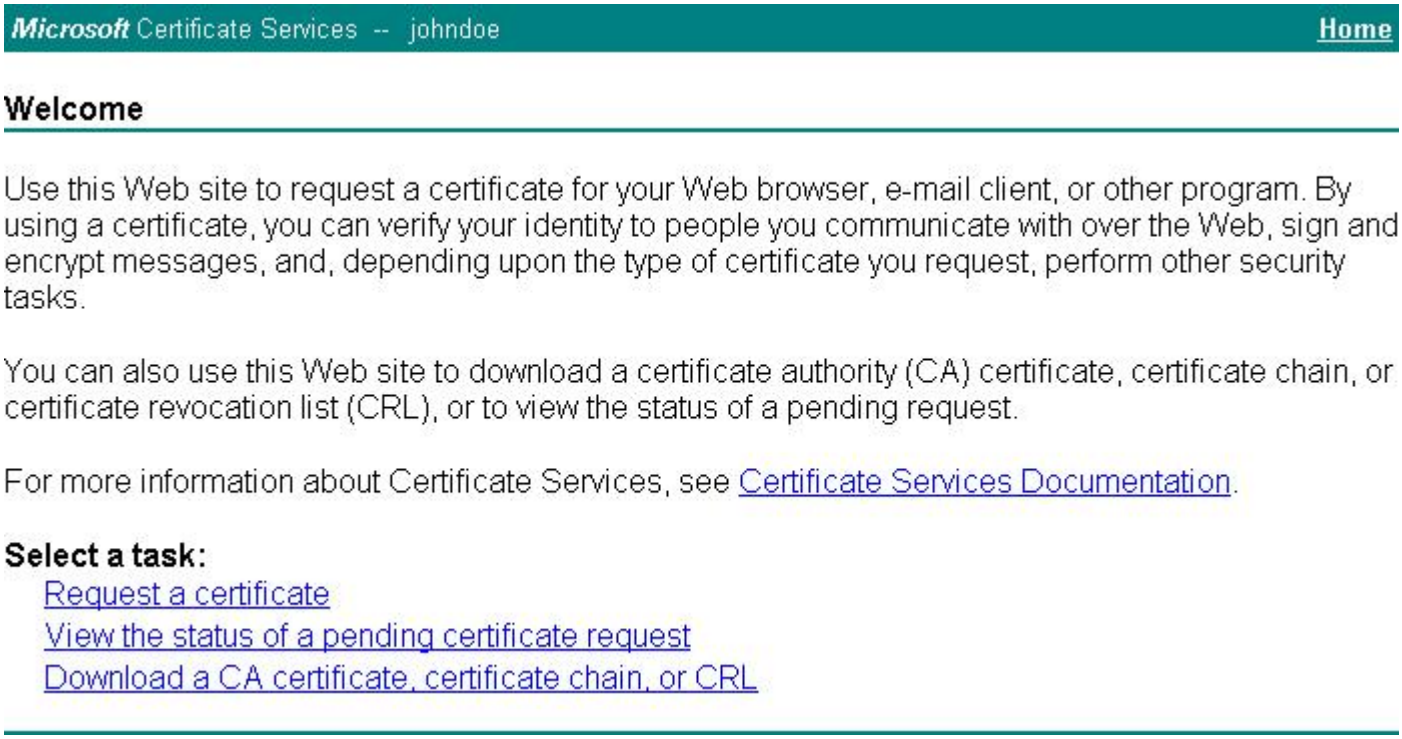
http://<CA IP address>/certsrv.

Sign into the CA with the username and password of the person who will be logging into the mobile device.



Logon to Certificate Authority

This process saves a user certificate and a separate private key file. Windows CE equipped devices such as the device require the private key to be saved as a separate file rather than including the private key in the user certificate.

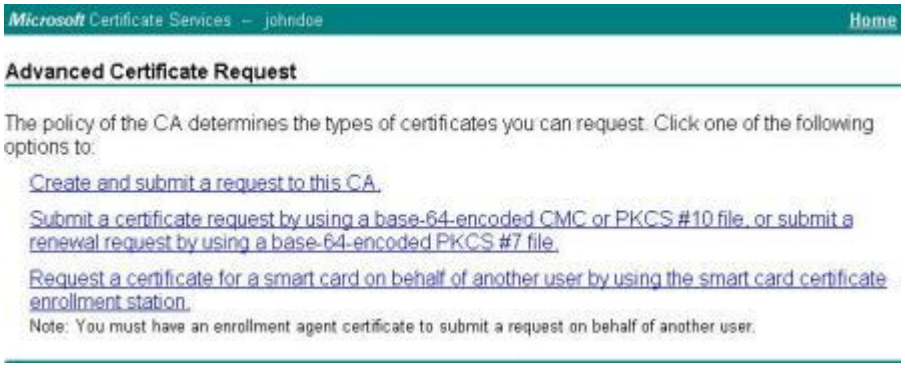

Microsoft Certificate Services -- johndoe
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Certificate Services Welcome Screen

Click the **Request a certificate** link.

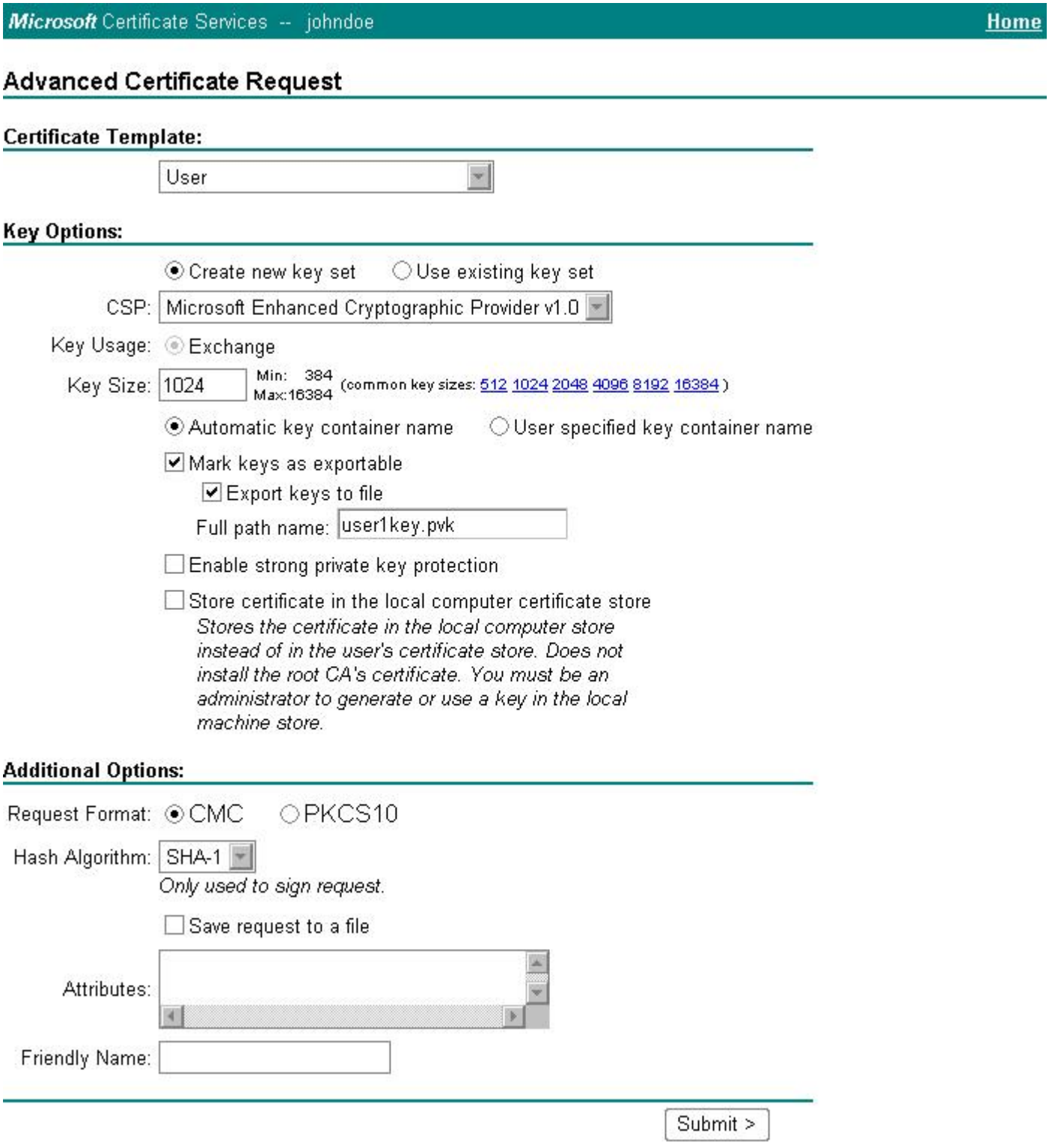
Request a Certificate Screen

Click on the **advanced certificate request** link.


Microsoft Certificate Services -- johndoe
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Advanced Certificate Request Screen

Click on the **Create and submit a request to this CA** link.



Advanced Certificate Details

For the **Certificate Template**, select **User**.

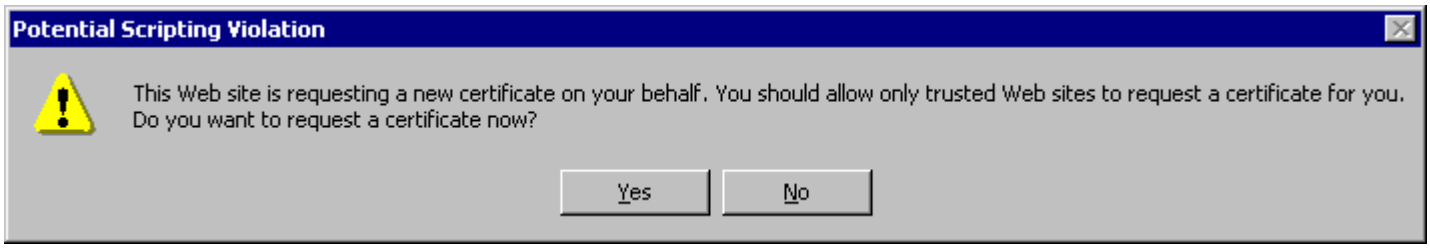
Check the **Mark keys as exportable** and the **Export keys to file** checkboxes.

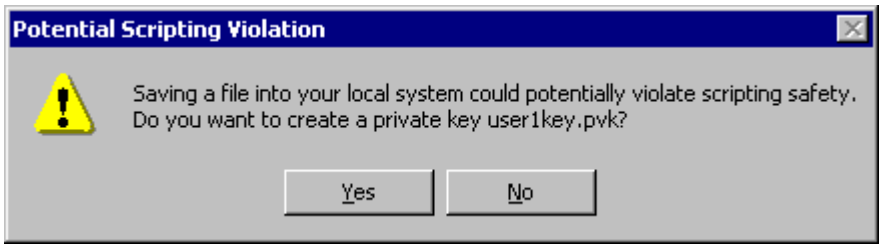
Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

Be sure to note the name used for the private key file, for example LXEUSER.PVK. The certificate file created later in this process must be given the same name, for example, LXEUSER.CER.

DO NOT check to use strong private key protection.

Make any other desired changes and click the **Submit** button.


Potential Scripting Violation
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?
Yes
No


Potential Scripting Violation
Saving a file into your local system could potentially violate scripting safety.
Do you want to create a private key user1key.pvk?
Yes
No

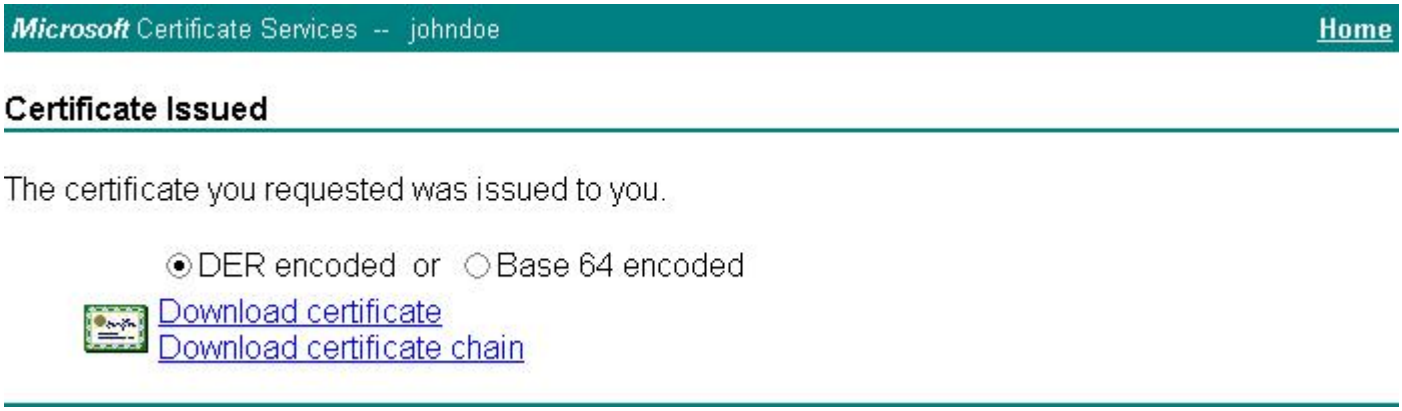
Script Warnings

If any script notifications occur, click the "**Yes** button to continue the certificate request.

Private Key Password

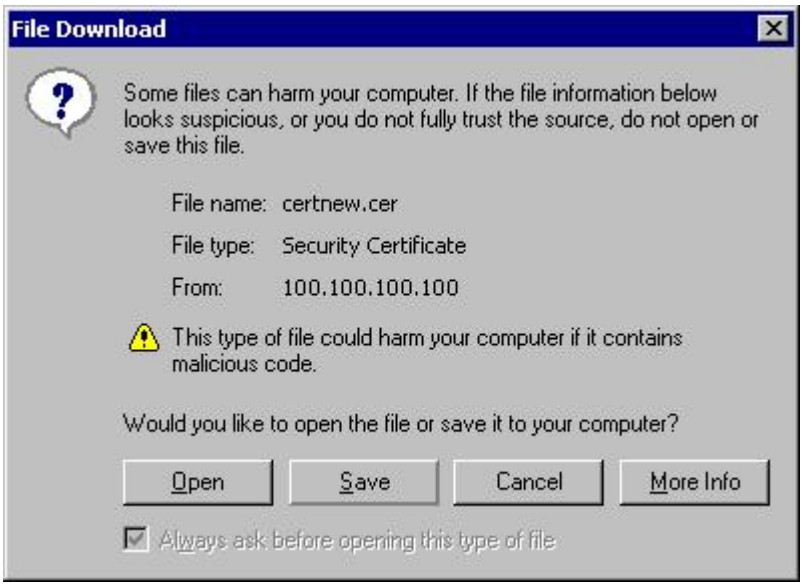
When prompted for the private key password:

- Click **None** if you do not wish to use a password, or
- Enter and confirm your desired password then click **OK**.



Certificate Issued

Click the **Download certificate** link.


File Download
Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
File name: certnew.cer
File type: Security Certificate
From: 100.100.100.100
This type of file could harm your computer if it contains malicious code.
Would you like to open the file or save it to your computer?
Open
Save
Cancel
More Info
Always ask before opening this type of file

Download Security Warning

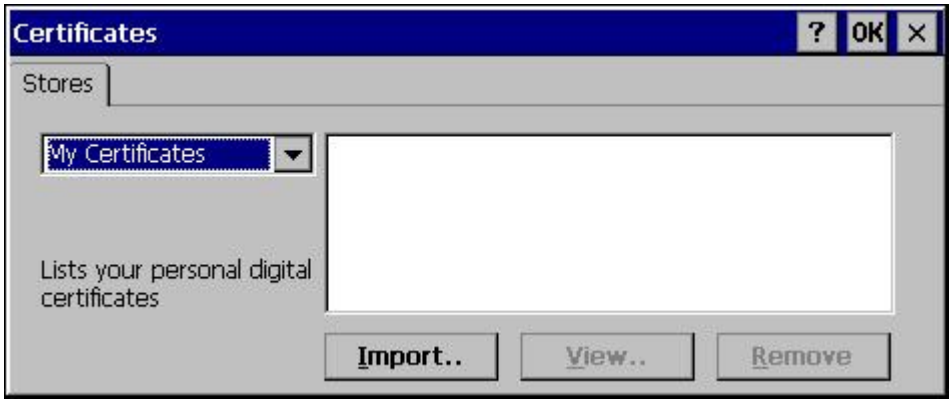
Click **Save** to download and store the user certificate to the PC. Make sure to keep track of the name and location of the certificate. The private key file is also downloaded and saved during this process.

Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as LXEUSER.PVK then the certificate file created must be given the same name, for example, LXEUSER.CER.

Installing a User Certificate

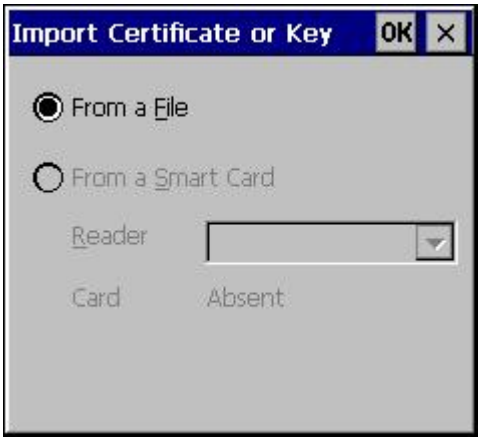
Copy the certificate and private key files to the MX9. Import the certificate by navigating to **Start | Control Panel | Certificates**.

Select **My Certificates** from the pull down list.



Certificates

Tap the **Import** button.

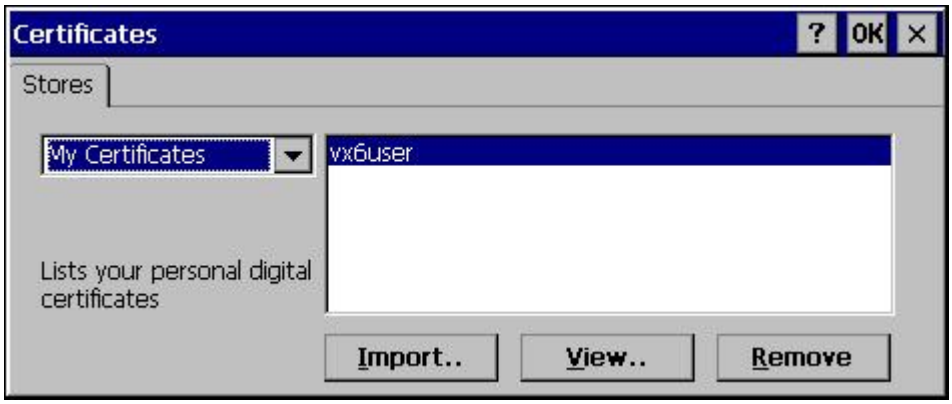


Import Certificate

Make sure **From a File** is selected and tap **OK**.

Browsing to Certificate Location

Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**. The certificate is now shown in the list.



Certificate Listing

With the certificate you just imported highlighted, tap **View**.

From the Field pull down menu, select **Private Key**.

Private Key Not Present

- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap **OK** to return to the Certificates screen.

Tap import.

Browsing to Private Key Location

Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to **Private Keys**, select the certificate desired and tap **OK**. Enter the password for the certificate if appropriate.

Tap on **View** to see the certificate details again.

Private Key Present

The private key should now say present. If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example LXEuser.cer for the certificate and LXEuser.pvk for the private key file. If the file names are not the same, rename the private key file and import it again.

Peripherals / Accessories

MX9 Accessories (PDF)

Carry Case

The handled and non-handled carry cases surround the MX9 while allowing user access to the touchscreen and keypad as well as an unobstructed view through the laser aperture.

The main battery can be removed and replaced without having to adjust the carrying case. The cases have a provision for retaining and tethering the stylus.

The cases have an integrated hand strap on the rear of the case for either left or right hand use. The cases have tether points for a removable shoulder strap. The shoulder strap allows the unit to hang upside down.

A removable, clear plastic protector for the keypad and display is provided as part of the non-handled and handled versions of the case.

Hand Strap

Once installed, the lightweight elastic hand strap provides a means for the user to secure the MX9 to their hand.

The hook and loop fabric strap is adjustable to fit practically any size hand. The bottom bracket must be slid out and away from the battery well when the main battery pack is being installed or replaced.

Note: Either the trigger handle is attached to the MX9 or the hand strap is attached, not both. LXE recommends that, in the absence of a trigger handle, the hand strap be used at all times.

Holster

A holster is available for the MX9 with a trigger handle and without a trigger handle.

The holsters can be worn on either the left or right side of the body and include a tether for retaining the stylus as well as a pocket for a spare battery.

The MX9 can be inserted and removed from the holster with a single motion without the need for a fastening strap to hold the MX9 in the holster.

The holsters are compatible with the LXE holster belt.

Stylus

The MX9 has a stylus that is stored in an elastic sleeve on the hand strap. Carry cases and holsters also have elastic sleeves for stylus storage.

The stylus can also be stored in a slot in the handle.

The stylus includes a tether that can withstand at least 5 pounds of pull force. The stylus can be used on the touch screen while tethered to the hand strap or handle.

Trigger Handle

The trigger handle is optional and can be ordered separately.

It is usable on all LXE hatch configurations and can be installed/removed by the end-user using common tools e.g. screwdriver.

The trigger handle has built-in storage for the touchscreen stylus and an integrated wrist strap.

The trigger on the handle is used to activate the integrated barcode decoder. The trigger can be remapped in the same manner as the keys on the keypad.

Note: Either the trigger handle is attached to the MX9 or the hand strap is attached, not both. LXE recommends that, in the absence of a trigger handle, the hand strap be used at all times.

Contact your LXE representative for the latest in upgrades and accessories.

Battery Multi-charger

The battery Multi-charger requires connection to an external power source before battery pack charging can commence. The AC power supply cable for the Multi-charger is not shipped with the multi-charger.

The battery pack begins to charge as soon as it is placed in any one of the four charging wells. Up to four fully drained main batteries can be fully charged in approximately four hours, simultaneously. The charging well LED indicates battery pack status. When the battery pack is inserted into the battery well, the retaining clip on the battery well snaps the battery securely into place in the battery well.

Remove the battery pack by first sliding the retaining clip away from the battery, then lifting the battery straight up and out of the battery well.

The Multi-charger has been designed for indoor use only. Do not operate outdoors or in extreme high humidity environments. Do not expose the Multi-charger to rain, snow or wet conditions.

Note: Do not "slam" or drop the battery into the charging well. Do not allow foreign material to fall or spill into the charging well. Failure to follow these instructions can result in damage to the main battery pack or the Multi-charger.

Status Indicators

Off	Battery pack not plugged in or no AC power applied
Flashing Red	Fault, battery pack fault or failure
Yellow / Amber	Standby, battery pack temperature out of range
Red	Charging, battery pack charging
Green	Battery pack fully charged

Multi-charger setup and use is covered in more detail in the MX9 Multi-charger User Guide.

Docking Cradles

Desktop Cradle

Note: Do not drop or slam the unit or the spare battery into the charging pockets. Damage to the contacts at the base of the charging pockets may result. Keep dirt and foreign objects out of the charging pockets. Do not short circuit any of the contacts in the charging pockets, as this action could result in injury or property damage.

The Desktop Cradle requires external AC power before battery charging and tethered scanning can commence. The cradle can simultaneously charge the main battery in the docked MX9 and charge a spare main battery.

A fully depleted spare battery recharges in approximately four hours in the powered cradle. When the MX9 is docked in the cradle, a spare battery can still be inserted in the spare battery charging pocket and both batteries are recharged at the same time.

Place the desktop cradle on a stable surface out of the way of:

- inclement weather conditions (water or high moisture),
- extremely high concentrations of dust or wind blown debris,
- accidental knocks, bumps or other shocks to the MX9 and the cradle.

Allow clearance above the cradle for an MX9 with a trigger handle for insertion ease. Allow clearance behind the cradle for cable connection ease. Route cradle cables to ensure they are protected from jostling, tugging or being disconnected by objects passing by.

Vehicle Cradle

Note: Do not drop or slam the unit into the docking bay. Damage to the contacts at the base of the charging/communication pocket may result. Keep dirt and foreign objects out of the charging pocket. Do not short circuit any of the contacts in the charging pocket, as this action could result in injury or property damage.

Using a cable adapter, the MX9 Vehicle Mount Cradle receives power from the vehicle's power supply. RAM ball vehicle mounting hardware is available that supports the MX9 cradle and mounts to overhead, dash, roof support pillars, and front screen positions on fork trucks or pallet jacks.

Vehicle input power,when secured to the vehicle cradle, passes to the MX9 in the docking bay. The MX9 operating system manages main battery charging, I/O interfaces through the connectors on the back of the cradle and all communication options.

For operation on a vehicle with greater than 12V, DC-DC accessory power supplies are available in 9-36V, 24-60V, and 60-150V ranges.

The vehicle's input power does not pass straight through to the MX9. The unconditioned 12V input power is boosted to 15V before being passed through to the MX9.

Cradle installation and use is covered in more detail in the MX9 Cradle Reference Guide.

KeyMaps

Introduction

The keypad is available in a 62-key or 38-key configuration.

The 62-key keypad is also available in an IBM 5250 configuration.

Notes:

- When using a sequence of keys that includes a sticky key, press the sticky key first, release it, then press the rest of the key sequence.
- Sticky keys do not need to be held down while pressing the next (or desired) key.
- When using a sequence of keys that includes the Orange or Blue keys, press the color key first then the rest of the key sequence.
- Alphabetic keys default to lower case letters. Press the Shft/Shift key, then the alphabetic key for an uppercase letter.

Note: In general, sticky keys refer to those keys that, when pressed once and released, are still in effect and affect the function of the next key pressed.

MX9 62-Key Keypad

A modifier key pressed after itself toggles that modifier key off.

Modifier keys pressed following any other modifier key clears earlier modifier keys.

Any key press, other than the up arrow or down arrow, exits the volume control and backlight control.

To get this function	Press these keys in this order			Result / Notes
Windows key	CTL	ESC		*Windows Start menu*
On (when Off)	Power			*Power On*
Suspend toggle (when On)	Power			*Suspend or Resume mode*
Volume Up	Orange	Right Scan	Up Arrow	*Volume increases*
Volume Up	Blue	V	Up Arrow	*Volume increases*
Volume Down	Orange	Right Scan	Down Arrow	*Volume decreases*
Volume Down	Blue	V	Down Arrow	*Volume decreases*
Display Backlight Lighter	Blue	Right Scan	Up Arrow	*Backlight lighter*
Display Backlight Darker	Blue	Right Scan	Down Arrow	*Backlight darker*
Alt mode	ALT			*Alt mode*
Ctl mode	CTL			*Control mode*
Escape	ESC			*Escape*
Space	SPC			*Space*
Enter	Enter			*Enter*
Capslock toggle	Blue	TAB		*Capslock is on or off*
Mapped Diamond 1 Key	Diamond 1			*Use the Keymap Control Panel to change default*

To get this function	Press these keys in this order			Result / Notes
Mapped Diamond 2 Key	Blue	Diamond 1		*Use the Keymap Control Panel to change default*
Uppercase Alpha toggle	SHFT			*Shifted letter*
Back space	BS (Backspace)			*Back one space*
Tab	TAB			*Tab*
Backtab	Orange	TAB		*Backtab*
Cursor Up	Up Arrow			*Cursor up one line*
Cursor Down	Down Arrow			*Cursor down one line*
Cursor Right	Blue	Up Arrow		*Cursor right one space*
Cursor Left	Blue	Down Arrow		*Cursor left one space*
Insert	Blue	I (letter i)		*Insert mode*
Insert	Orange	CTL		*Insert mode*
Delete	Orange	BS		*Delete one character*
Home	Orange	SHFT	Down Arrow	*Home*
End	Orange	SHFT	Up Arrow	*End*
Page up	Orange	Up Arrow		*Up 1 screen*
Page down	Orange	Down Arrow		*Down 1 screen*
F1	F1			*F1 mode*
F2	F2			*F2 mode*
F3	F3			*F3 mode*
F4	F4			*F4 mode*
F5	F5			*F5 mode*
F6	F6			*F6 mode*
F7	F7			*F7 mode*
F8	F8			*F8 mode*
F9	F9			*F9 mode*
F10	F10			*F10 mode*
F11	Blue	F1		*F11 mode*
F12	Blue	F2		*F12 mode*
F13	Blue	F3		*F13 mode*
F14	Blue	F4		*F14 mode*
F15	Blue	F5		*F15 mode*
F16	Blue	F6		*F16 mode*
F17	Blue	F7		*F17 mode*

To get this function	Press these keys in this order			Result / Notes
F18	Blue	F8		*F18 mode*
F19	Blue	F9		*F19 mode*
F20	Blue	F10		*F20 mode*
F21	SHFT	F1		*F21 mode*
F22	SHFT	F2		*F22 mode*
F23	SHFT	F3		*F23 mode*
F24	SHFT	F4		*F24 mode*
a	A			*a (lowercase is the default)*
b	B			*b*
c	C			*c*
d	D			*d*
e	E			*e*
f	F			*f*
g	G			*g*
h	H			*h*
i	I			*i*
j	J			*j*
k	K			*k*
l	L			*l*
m	M			*m*
n	N			*n*
o	O			*o*
p	P			*p*
q	Q			*q*
r	R			*r*
s	S			*s*
t	T			*t*
u	U			*u*
v	V			*v*
w	W			*w*
x	X			*x*
y	Y			*y*
z	Z			*z*
A	SHFT	A		*A*
B	SHFT	B		*B*
C	SHFT	C		*C*

To get this function	Press these keys in this order			Result / Notes
D	SHFT	D		*D*
E	SHFT	E		*E*
F	SHFT	F		*F*
G	SHFT	G		*G*
H	SHFT	H		*H*
I	SHFT	I		*I*
J	SHFT	J		*J*
K	SHFT	K		*K*
L	SHFT	L		*L*
M	SHFT	M		*M*
N	SHFT	N		*N*
O	SHFT	O		*O*
P	SHFT	P		*P*
Q	SHFT	Q		*Q*
R	SHFT	R		*R*
S	SHFT	S		*S*
T	SHFT	T		*T*
U	SHFT	U		*U*
V	SHFT	V		*V*
W	SHFT	W		*W*
X	SHFT	X		*X*
Y	SHFT	Y		*Y*
Z	SHFT	Z		*Z*
1	1			*1*
2	2			*2*
3	3			*3*
4	4			*4*
5	5			*5*
6	6			*6*
7	7			*7*
8	8			*8*
9	9			*9*
0 (zero)	0			*0 (zero)*
. (period)	Orange	SPC		*Period*
. (period)	Orange	K		*Period*
-	Blue	SPC		*Dash or minus sign*
/	Blue	J		*Reverse Solidus or*

To get this function	Press these keys in this order			Result / Notes
				Backslash
\	Orange	S		*Solidus or Forward slash*
[	Blue	Y		*Left square bracket*
]	Blue	Z		*Right square bracket*
'	Orange	N		*Acute accent or single quote or apostrophe*
,	Orange	J		*Comma*
;	Orange	F		*Semicolon*
=	Blue	T		*Equal sign*
!	Orange	Q		*Exclamation mark*
!	SHFT	1 (number)		*Exclamation mark*
@	Orange	W		*At sign*
@	SHFT	2 (number)		*At sign*
#	Orange	E		*Number sign*
#	SHFT	3 (number		*Number sign*
$	Orange	R		*Dollar sign*
$	SHFT	4 (number)		*Dollar sign*
%	Orange	T		*Percent sign*
%	SHFT	5 (number)		*Percent sign*
^	Orange	Y		*Caret or circumflex*
^	SHFT	6 (number)		*Caret or circumflex*
&	Orange	U		*Ampersand*
&	SHFT	7 (number)		*Ampersand*
*	Orange	I (alpha i)		*Asterisk*
*	SHFT	8 (number)		*Asterisk*
(	Orange	O (alpha o)		*Left parenthesis*
(	SHFT	9 (number)		*Right parenthesis*
)	Orange	P		*Left parenthesis*
)	SHFT	0 (zero)		*Right parenthesis*
"	Orange	G		*Double quote*
{	Blue	W		*Curly left brace*
}	Blue	X		*Curly right brace*
|	Orange	A		*Vertical bar or Pipe*
~	Orange	B		*Tilde*
<	Blue	G		*Less than mark*
>	Blue	H		*Greater than mark*

To get this function	Press these keys in this order			Result / Notes
:	Orange	D		*Colon*
+	Blue	BS (Backspace)		*Plus sign*
?	Orange	L		*Question mark*
_	Orange	M		*Underscore or horizontal bar*
Enter	ENTER			*Enter*

KeyMaps 62-Key 5250 Overlay

Legend	Explanation	Key Sequence
Attn	Attention	CTL + A
Clr	Clear	CTL + C
Del	Delete	CTL + D
Dup	Duplicate	CTL + U
E-Inp	Erase Input	CTL + Q
Field Exit	Enter	Diamond 1
Fld -	Field Minus	CTL + M
Fld +	Field Plus	CTL + L
Ins	Insert	CTL + I
NL	New Line	CTL + N
SysReq	System	CTL + S

See Also: Key Map for 62 Key Keypad

MX9 38-key Keypad

A modifier key pressed after itself toggles that modifier key off.

Any key press, other than a modifier key following any modifier key *unsticks* the modifier keys.

Any key press, other than up or down arrow, exits volume control mode or backlight control mode

To get this function	Press these keys in this order			Result / Notes
Windows key	CTRL	Esc		*Windows Start menu*
On (when Off)	Power			*Power On*
Suspend toggle (when On)	Power			*Suspend or Resume mode*
Volume Up	Orange	Right Scan	Up Arrow	*Volume increases*
Volume Down	Orange	Right Scan	Down Arrow	*Volume decreases*
Display Backlight Lighter	Blue	Right Scan	Up Arrow	*Backlight lighter*
Display Backlight Darker	Blue	Right Scan	Down Arrow	*Backlight darker*
Scan (Right)	Right Scan			*Activate decoder*
Scan (Left)	Left Scan			*Activate decoder*
Alt mode	ALT			*Alt mode*
Ctrl mode	CTRL			*Control mode*
Escape	Esc			*Escape*
Space	SPC			*Space*
Enter	Enter			*Enter*
Capslock toggle	Blue	TAB		*Capslock is on or off*
Mapped Diamond 1 Key	Diamond 1			*Use the Keymap Control Panel to change default*

To get this function	Press these keys in this order			Result / Notes
Mapped Diamond 2 Key	Diamond 2			*Use the Keymap Control Panel to change default*
Uppercase Alpha toggle	SHIFT			*Shifted letter*
Back space	BKSP			*Back one space*
Tab	TAB			*Tab*
Backtab	Orange	TAB		*Backtab*
Cursor Up	Up Arrow			*Cursor up one line*
Cursor Down	Down Arrow			*Cursor down one line*
Cursor Right	Blue	Up Arrow		*Cursor right one space*
Cursor Left	Blue	Down Arrow		*Cursor left one space*
Insert	Orange	CTRL		*Insert mode*
Delete	Orange	BKSP		*Delete one character*
Home	Orange	SHIFT	Down Arrow	*Home*
End	Orange	SHIFT	Up Arrow	*End*
Page up	Orange	Up Arrow		*Up 1 screen*
Page down	Orange	Down Arrow		*Down 1 screen*
F1	F1			*F1 mode*
F2	F2			*F2 mode*
F3	F3			*F3 mode*
F4	F4			*F4 mode*
F5	F5			*F5 mode*
F6	F6			*F6 mode*
F7	F7			*F7 mode*
F8	F8			*F8 mode*
F9	F9			*F9 mode*
F10	F10			*F10 mode*
F11	Blue	F1		*F11 mode*
F12	Blue	F2		*F12 mode*
F13	Blue	F3		*F13 mode*
F14	Blue	F4		*F14 mode*
F15	Blue	F5		*F15 mode*
F17	Blue	F7		*F17 mode*
F18	Blue	F8		*F18 mode*
F19	Blue	F9		*F19 mode*
F20	Blue	F10		*F20 mode*

To get this function	Press these keys in this order			Result / Notes
F21	SHIFT	F1		*F21 mode*
F22	SHIFT	F2		*F22 mode*
F23	SHIFT	F3		*F23 mode*
F24	SHIFT	F4		*F24 mode*
a	Alpha	2		*a*
b	Alpha	22		*b*
c	Alpha	222		*c*
d	Alpha	3		*d*
e	Alpha	33		*e*
f	Alpha	333		*f*
g	Alpha	4		*g*
h	Alpha	44		*h*
i	Alpha	444		*i*
j	Alpha	5		*j*
k	Alpha	55		*k*
l	Alpha	555		*l*
m	Alpha	6		*m*
n	Alpha	66		*n*
o	Alpha	666		*o*
p	Alpha	7		*p*
q	Alpha	77		*q*
r	Alpha	777		*r*
s	Alpha	7777		*s*
t	Alpha	8		*t*
u	Alpha	88		*u*
v	Alpha	888		*v*
w	Alpha	9		*w*
x	Alpha	99		*x*
y	Alpha	999		*y*
z	Alpha	9999		*z*
A	SHFT	Alpha	2	*A*
B	SHFT	Alpha	22	*B*
C	SHFT	Alpha	222	*C*
D	SHFT	Alpha	3	*D*
E	SHFT	Alpha	33	*E*
F	SHFT	Alpha	333	*F*
G	SHFT	Alpha	4	*G*

To get this function	Press these keys in this order			Result / Notes
H	SHFT	Alpha	44	*H*
I	SHFT	Alpha	444	*I*
J	SHFT	Alpha	5	*J*
K	SHFT	Alpha	55	*K*
L	SHFT	Alpha	555	*L*
M	SHFT	Alpha	6	*M*
N	SHFT	Alpha	66	*N*
O	SHFT	Alpha	666	*O*
P	SHFT	Alpha	7	*P*
Q	SHFT	Alpha	77	*Q*
R	SHFT	Alpha	777	*R*
S	SHFT	Alpha	7777	*S*
T	SHFT	Alpha	8	*T*
U	SHFT	Alpha	88	*U*
V	SHFT	Alpha	888	*V*
W	SHFT	Alpha	9	*W*
X	SHFT	Alpha	99	*X*
Y	SHFT	Alpha	999	*Y*
Z	SHFT	Alpha	9999	*Z*
1	1			*1*
2	2			*2*
3	3			*3*
4	4			*4*
5	5			*5*
6	6			*6*
7	7			*7*
8	8			*8*
9	9			*9*
0 (zero)	0			*0 (zero)*
. (period)	Orange	SPC		*Period*
-	Blue	SPC		*Dash or minus sign*
/	Blue	1		*Reverse Solidus or Backslash*
****	Orange	1		*Solidus or Forward slash*
[	Orange	2		*Left square bracket*
[	Blue	2		*Left square bracket*

To get this function	Press these keys in this order			Result / Notes
]	Orange	3		*Right square bracket*
]	Blue	3		*Right square bracket*
'	Orange	Alpha		*Acute sign or single quote or apostrophe*
,	Orange	6		*Comma*
;	Blue	0 (zero)		*Semicolon*
=	Orange	Esc		*Equal sign*
!	Blue	ALT		*Exclamation mark*
!	SHFT	1 (number)		*Exclamation mark*
@	Orange	5		*At sign*
@	SHFT	2 (number)		*At sign*
#	Orange	4		*Number sign*
#	SHFT	3 (number)		*Number sign*
$	Orange	9		*Dollar sign*
$	SHFT	4 (number)		*Dollar sign*
%	SHFT	5 (number)		*Percent sign*
^	Blue	CTRL		*Caret or circumflex*
^	SHFT	6 (number)		*Caret or circumflex*
&	SHFT	7 (number)		*Ampersand*
*	Orange	Diamond 1		*Asterisk*
*	SHFT	8 (number)		*Asterisk*
(	Blue	Esc		*Left parenthesis*
(	SHFT	9 (number)		*Right parenthesis*
)	Blue	SHIFT		*Left parenthesis*
)	SHIFT	0 (zero)		*Right parenthesis*
"	Blue	Alpha		*Double quote*
{	Blue	4		*Curly left brace*
}	Blue	5		*Curly right brace*
|	Orange	ALT		*Vertical bar*
~	Blue	9		*Tilde*
<	Blue	7		*Less than mark*
>	Blue	8		*More than mark*
:	Orange	0 (zero)		*Colon*
+	Blue	BKSP (Backspace)		*Plus sign*
?	Orange	8		*Question mark*
_	Orange	7		*Underscore or horizontal bar*

Technical Specifications

MX9

Processor	Marvell PXA-320 / 806 MHz
Memory	128MB on-board RAM / 128 on-board Flash
Expansion slots	SD expansion slot for flash memory (128MB / 512MB / 1GB / and 4 GB supported) Internal CF slot for Summit a/b/g radio, protected inside device.
Operating System	Microsoft Windows CE 5.0
Radio Modules	802.11 a/b/g radio / WWAN / SuperRaptor radio / Bluetooth / GPS receiver
Integrated Scanner / Imager	SE955 standard range scan engine or replacement SE1524 Lorax scan engine HHP 5300SF imager
Display technology	TFT / Active Matrix / Transflective / LED backlight
Touch screen actuation force	10 grams min to 80 grams max
Standard Battery	2400mAhr (room temperature)
Low Temperature Battery	2200mAhr (room temperature)
Backup Power	SuperCap is used for backup, no backup "battery" is used.
External I/O Port Functions	External Power In USB Host USB Client| RS232 RS232 w/5V 4-wire Audio 10/100 BaseT Ethernet (Ethernet port available in cradle)
Internal I/O Ports	One serial port (DTE) with appropriate power for a WAN radio One serial port (DTE) for an integrated laser decoder USB 1.1 Host (capable) with power (5V @ 500mA) One SSP port (capable) One SD port for I/O expansion (capable) One SIM port for WAN One serial port (DTE) for interface with GPS receiver chip One camera port for non-decoding imager

Dimensions and Weight

Dimensions and weights for MX9 configurations.

Length (overall)	9.94 in / 25.2 cm
Width at Display	3.87 in / 9.8 cm
Depth at display/scanner	2.67 in / 6.8 cm
Width at keypad	2.94 in / 7.5 cm
Depth at keypad	1.78 in / 4.5 cm
Configured with battery, scanner, Bluetooth, 802.11x radio, handstrap and stylus	34.75 oz / .9.85 kg
Configured with battery, Bluetooth, handstrap and stylus	30.6 oz / .87 kg
Configured with battery, scanner, Bluetooth, 802.11x radio, trigger handle and stylus	37.83 oz / .1.072 kg

Environmental Specifications

Standard Operating Temperature	-4°F to 140°F (-20°C to 60°C) [non-condensing]
Freezer Operating Temperature	-22°F to 140°F (-30°C to 60°C) [with heater or other additions as required]
Storage Temperature	-4°F to 158°F (-20°C to 70°C) [non-condensing]
Operating Humidity	5% to 95% non-condensing. This does not apply to cold storage areas where condensation will appear.
Water and Dust	IEC 60529 compliant to IP67
Vibration	Based on MIL Std 810D
Bluetooth Range	32.8 feet (10 meters) Direct line of sight only

Main Battery Technical Specifications

Standard Battery Operating Temperature Range	-20°C to + 60°C (-4°F to 140°F) non-condensing
Standard Battery Storage Temperature Range	-20°C to + 70°C (-4°F to 158°F) to non-condensing
Low Temperature Battery Operating Temperature Range	-30°C to + 60°C (-22°F to 140°F) non-condensing
Low Temperature Battery Storage Temperature Range	-30°C to + 70°C (-22°F to 158°F) non-condensing
Operating Humidity	5% to 95% non-condensing at 40°C (104°F)
Ingress Protection Enclosure Rating	Compliant to IP67
Charge Cycles	500 minimum
Discharge Time (Average)	Standard: 8 hours Low Temperature: 5 hours
Discharge Current (Average)	< 300mA
Charging low-voltage cut-off	3.9A nominal

Wireless Radio

Two wireless radios are available:

- Summit CF 802.11b/g (2.4GHz)
- Summit CF 802.11a/b/g (5 GHz)

These radios support antenna diversity and are WiFi certified.

For 2.4 GHz frequency band, the site survey limit is -75 dBm signal strength, 15 dB SNR as measured by LXE.

For 5 GHz frequency band, the site survey limit is -65 dBm signal strength, 15 dB SNR as measured by LXE.

The noise levels for each of the radios (as measured by the MX9 appropriate antenna) is less than or equal to the values specified in the table below for the frequency band specified:

WLAN Radio Type	**Noise Level (dBm)**	**Channel Bandwidth**	**Frequency Band**
802.11 b/g	-95 dBm	20 MHz	2.4 GHz - 2.483 GHz
802.11a/b/g	- 85 dBm	20 MHz	5.15-5.35GHz (FCC UNII 1 and UNII 2), 5.725-5.825GHz (FCC UNII 3)

Bluetooth System Compatibility

Bluetooth specification Version 2.0 + EDR . Supports Bluetooth Enhanced Data Rate (EDR)

- Supports UART
- Class 2 – 2.5mW (4dBm) output power
- Supports the 921 kbps baud rate
- Adaptive Frequency Hopping – AFH
- Backward compatibility with Bluetooth 1.1 and 1.2

WWAN Radio

Note: Only one radio at a time can be in an MX9.

The MX9 provides an 802.11a/b/g WWAN radio and supports GSM/EDGE.

Carriers are AT&T in the US (GSM) and RTTE Europe.

GSM radios are shipped on deactivated SIM cards.

AC/DC Wall Adapter

The AC/DC Power Adapter is only intended for use in a 25°C (77°F) maximum ambient temperature environment.

Input Power Switch	None
Power "ON" Indicator	LED
Input Fusing	Thermal Fuse
Input Voltage	100 VAC min – 240 VAC max
Input Frequency	50 - 60 Hz
Input Connector	Three prong wall plug with ground
Output Connector	AC wall adapter has a 5.5mm barrel connector. It connects to the I/O cables which transition power to the D connector.
Output Voltage	15 VDC
Output Current	4 Amps max
Output Power	60 Watt max
Charging low-voltage cut-off	3.9A nominal
Operating Temperature	32° F to 100° F / -0° C to 40° C
Storage Temperature	-4° F to 140° F / -20° C to 60° C
Weight	250 grams

GPS Receiver Technical Specifications

The GPS receiver COM port is turned off by default. The COM port is 5, defaults are 9600 baud, 8 bits, no parity, 1 stop bit. COM5 default baud rate is 4800 for NMEA communication. GPS COM settings are stored in the registry.

Frequency Band

Channel bandwidth is 2 MHz. Frequency band is 1574.42 GHz to 1576.42 GHz.

Serial Interface

The GPS module supports serial interface for data communication. Transmission (TX) and Reception (RX) signals are implemented to send commands and to receive GPS data. LXE designs use UART B on the module for communication.

The default baud rate for the NMEA 0183 protocol is 9600 bps, 8 bits, Parity None, 1 Stop. The baud rate can be increased to 115Kbps.

Accuracy

Position to within 10 meters, 2D Root Mean Square (RMS) and 5 meters 2D RMS, Satellite Based Augmentation System (SBAS) corrected.

Velocity to within 24 meters per second.

SBAS is compatible with the Wide Area Augmentation System (WAAS) satellite signal augmenter (United States) and the EGNOS satellite signal augmenter (Europe).

Protocol

The module outputs the following messages:

- GGA - GPS Fix Data
- RMS - Recommended Minimum Specific GPS Data
- GSA - GPS DOP and Active Satellites
- GSV - GPS Satellites in View
- GLL - Geographic Position Latitude/Longitude
- VTG - Course over Ground and Ground Speed.

The GPS module supports NMEA 0183 protocol and SiRF Binary Protocol.

AppLock Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter…" is logged at the beginning of the function specified in the message and "Exit…" is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_ PROCESSING
App= <Application name>	Name of the application being locked	LOG_ PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX
**********	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_ PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_ PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_ PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_ PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_ PROCESSING
Enter password timeout	Entering the password timeout processing.	LOG_ PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_ PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_ PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_ PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_ PROCESSING
Enter verify password	Entering the password verification processing.	LOG_ PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_ PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_ PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_

Message	Explanation and/or corrective action	Level
		PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_ PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_ PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_ PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_ PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_ PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_ PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_ PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_ PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_ PROCESSING
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_ PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_ PROCESSING
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_ PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_ PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_ PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_ PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_ PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_ PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR

Message	Explanation and/or corrective action	Level
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_ PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_ WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_ PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_ PROCESSING
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_ PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_ PROCESSING
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_ PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_ PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_ PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_ PROCESSING
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_ PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_ PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_ PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX

Message	Explanation and/or corrective action	Level
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock's control of the taskbar should be removed.	LOG_EX
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

Hat Encoding

Hat Encoded Characters Hex 00 through AD

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~'
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

Hat Encoded Characters Hex AE through FF

Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

Desired ASCII	Hex Value	Hat Encoded
Ù	DB	~[
Ú	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

Revision History

Revision / Date	Location	Change
A / Aug 2009 - Initial Release		
B / Sep 2009	1. Cover page and contents 2. Components 3. Peripherals	1. Marketing color scheme. 2. Added missing photos. 3. Added links to Cradle Reference Guide and Battery Multi-charger User Guide
C/ Dec 2009	Control Panel - Admin-istration	Troubleshooting: Removed AppLock back door key sequence.

Index

3

38-key Keymaps ... 267

6

62-key 5250 Overlay Key Sequences ... 266
62-key Keymaps ... 260

A

About ... 52, 195
About Tab ... 141
AC/DC 15V Power Supply ... 20
Accessibility ... 54
ActiveSync ... 41
ActiveSync Introduction ... 35
Add Prefix ... 107
Add Suffix ... 107
Admin ... 194
Admin Hotkey
  AppLock ... 58
Admin Login ... 203
Admin Password ... 221
Advanced Button ... 102
Aggressive Scan ... 217
AimTimer ... 140
Allow Close ... 67
Alpha key
  38-key keypad ... 267
Alpha mode Status LED ... 15
Antenna
  Diversity
    Receive ... 219
    Transmit ... 218
API calls ... 31
Appearance ... 146
AppLock
  End-user mode ... 59
  EUIE ... 68
  Hotkey for Administrator ... 58
  Passwords ... 59
  Setup ... 55
Assign ... 133
Auth Server ... 218
Auth Timeout ... 221
Authentication ... 198
Auto-reconnect, Bluetooth ... 89
Auto hide ... 38
Auto Profile ... 204
Autoconnect ... 194
Automatic reset ... 54

B

Background ... 145
Backlight ... 146
Backlight setting is synchronized ... 178
backup battery ... 73
Barcode Data Match Edit Buttons ... 105
Barcode manipulation parameter settings ... 91
Barcode processing ... 93
Barcode Processing Examples ... 137
Barcode Readers ... 92
Battery ... 73
battery gas gauge icon ... 73
Battery Multi-charger ... 257
Battery State and OS Upgrade ... 197
Battery Status LED ... 15
Battery Technical Specifications ... 274
BG Channel Set ... 216
Bit Rate ... 208
Bluetooth
  About panel ... 82
Bluetooth Beep and LED Indications ... 89
Bluetooth Client Barcode Decoders
  Compatible ... 18

Bluetooth client functions 15
Bluetooth control panel 74
Bluetooth Device 75
Bluetooth Device Menu 77
Bluetooth Device Properties 78
Bluetooth Indicators 85
Bluetooth Properties panel 78
Bluetooth Status LED 15
Bluetooth System Compatibility 275
Bottom 5

C

CAB Files on the Flash Card 31
Cables 17
Calibration 184
Car Power Adapter 20
Carry Case 256
CCX Features 217
Centering 139
Certificates 90, 242
  Root CA 242
  User 247
Certs 35
Certs Path 222
Character Recognition
  Touchscreen 37
CLA Fuse 20
Clear All button 135
Clear Button 103
Clear Contents of Document Folder 39
Clear persistant memory 26
Client Name 207
Codabar 109, 117
Code IDs 134
Code11 110, 118
Code128 123
Code39 111, 119, 123
Code93 123
Cold Storage 17
COM Ports 13
COM1 Tab 96
Command Prompt 36
Communication 166
Component Diagrams 2
Components
  Back 6
  Labels 9
Computer Friendly Name 82
Configuration
  AppLock 61
Configuring the Profile 227
Connect and LXEConnect 35
Connection 192
Control Char mapping 100
Control Code Replacement 136
Control Panel options 50
Cradle 258
Critical Suspend Power State 24
Ctrl Char Mapping 132
Custom AIM IDs 108
custom Code IDs 134
Custom identifier 100
Custom Identifiers 134

D

Data Options Tab 98
Data stripping 104
Date, Time, Time Zone 143
Daylight Savings 143
DecodeMode 139
Default Input Language 152
Desktop 32
Desktop Cradle 258
DFS Channels 217
Diags Tab 213
Dialing 144
Dimensions and Weight 273
Discover 76

Discover and Query 76
Display 144
Diversity
  Receive 219
  Transmit 218
Double Tap 184

E

EAN13 121
  Mesa 123
EAN8 120
EAP-FAST 198
EAP-TLS 198
EAP Type 210
Enable Code ID drop down box 99
Encryption 198
Environmental Specifications 273
Error Messages
  AppLock 277
EUIE 68
Expand Control Panel 39
Expansion Slots 13
External Input/Output Port 12
External Power Supplies 19

F

Factory Default 182
Factory Default Settings 94
Factory Default Settings - AppLock 56
Factory Default, reset to 26
Flashlight 176
Frag Thresh 219
Front 2
FTP Server, start and stop 35

G

Global Parameters 214
Global Tab 214
Good Scan and Bad Scan Sounds 190
GPS 177
  Power Consumption, Serial Interface, Accuracy, Protocol 18
GPS Module
  Power Consumption 18

H

Handstrap 8
Headset 159
Heaters 175
Heating Elements 17
Help 199
HHP Custom IDs 115
HHP Properties 138
Hide Password 221
High Contrast 54
Holster 256
Holster Belt 256
Hotkey
  AppLock 69

I

Icons
  Explorer, Internet 32
  My Computer 32
  My Documents 32
  Recycle Bin 32
Identifying Software Versions 53
Imager aperture 5
Input / Output Connector 5
Input Panel 148, 159
Integrated Barcode Decoders
  Compatible 18
Interleaved 2 of 5 112, 122-123
Internal Scanner Sound 97
Internet 149
Internet connectivity 149
Internet Explorer
  AppLock 68
  Radio card and ISP required 36

Introduction
Main 1

J

Jacked 73

K

Key sequences
38-key keypad 267
62-key keypad 260
Keyboard 152
Shortcuts 25
KeyMap 153
KeyMap Tab 154
Keymapping 259
Keypads 13

L

Language and Fonts 52
LAUNCH.EXE 29
LaunchApp Tab 156
Leading and Trailing 104
LEAP 198
LeaveLightsOn 140
LED 220
Alpha Mode 15
Battery Multi-charger 257
Battery Status 15
Bluetooth 15
System Status 15
LEDs (Light Emitting Diodes) 15
Length Based Barcode Stripping 142
LinearRange 140
Load Factory Defaults 182
Load User Defaults 182
Logging
AppLock 72

M

MAC Address 53
Main Battery 19
main battery status 15
Main Tab 95, 202
Match Edit Buttons 105
Match List Rules 106
Media Player 36
Menu Options
Start 34
Mesa 123
Misc 168
Mixer 158
Modes
AppLock 58
Modifier Keys 13
Mouse 160
MouseKeys 54
MSI 113, 124

N

NDISlog 165
Network 192
Network and Dialup Options 161
Network Capture 163
No Security 228
Notification 54
Notification Tab 97

O

OCR 125
Off 24
Output panel 159
Owner 170

P

Password 172
AppLock 59

AppLock Save As ... 72
PC Connection ... 174
PEAP-GTC ... 198
PEAP-MSCHAP ... 198
PEAP/GTC ... 233
Summit Radio ... 233, 238
PEAP/MSCHAP
Summit Radio ... 231
Peripherals ... 175
Peripherals / Accessories ... 256
Permanent storage of drivers and utilities ... 31
Ping Delay ms ... 222
Ping Payload ... 222
Ping Timeout ms ... 222
Planet ... 126
Posicode ... 127
Power ... 178
Power Key Functions ... 14
power management status ... 15
Power Modes
On, Suspend, Off ... 21
Power modes, explained ... 14
Power On/Off key ... 14
Power Save ... 207
power up password ... 172
Pre-loaded Files ... 29
Prefix / Suffix ... 107
PREGEDIT.EXE ... 30
Profile ... 207
Profile Parameters ... 207
Profile Tab ... 205
Prompt
Command ... 36

R

Radio Mode ... 209
RAS (Remote Access Services) ... 162
Recalibrate button ... 184
Reflash ... 196
Introduction ... 196
Regional and Language Settings ... 180
Registry ... 52, 182
Registry content
back up location ... 31
Registry Editor ... 52
REGLOAD.EXE ... 30
Remote desktop connection ... 37
Remove button ... 135
Remove Programs ... 183
Replace CLA Fuse ... 20
Revision History ... 285
Roam Delta ... 215
Roam Period ... 216
Roam Trigger ... 215
Root CA Certificates
Generating ... 242
Installing on MX9 ... 245
RSS and Composite ... 115
RTS Thresh ... 220
RunCmd Tab ... 157
RX Diversity ... 219

S

Save User Defaults ... 182
Scanner aperture ... 5
Scanner Status LED ... 16
Scanners and Imagers
Compatible ... 18
screensaver password ... 173
Security Panel
AppLock ... 69
Security Password
AppLock ... 69
Serial Port Pin 9 ... 96
Settings ... 79
Setup
AppLock ... 55

Show Clock 38
Sign-On vs. Stored Credentials 223
SIM cards 275
Software and Files 29
SoundSentry 54
Speaker volume decibel level 159
Special Purpose Keys - 38 Key 4
Special Purpose Keys - 62 Key 3
SSID 207
Start Menu 34
Status LEDs 15
  Multi-charger 257
Status Panel
  AppLock 71
Status Popup 169
Status Tab 212
StickyKeys 54
Strip Leading/Trailing Control 104
stylus 184
Stylus 184, 256
Stylus storage bay in handle 7
Subsequent Use 84
Summit 35
Summit CF 802.11a/b/g 274
Summit CF 802.11b/g 274
Summit Client Utility 199
Summit Tray Icon 200
Suspend
  Power State 23
Suspend Primary Wake up Events 23
Symbologies 108
Symbologies dialog 101
Symbology Parameters 103
Symbology settings 100
Symbology Settings 100
Sync button 143
System 184
System Hardware 10
System Idle Power State 22
System Idle timer 178
System Status LED 15

T

TCP/IP 193
Telepen 128
Temperature and Humidity 273
Terminal Server Client Licenses 188
Tethered Barcode Decoders
  Compatible 18
ToggleKeys 54
Top 5
Transcriber 37
Tray Icon 220
Trigger Handle 7, 256
Troubleshooting 197
  Reflash 197
Turn Off Bluetooth 79
TX Diversity 218
Tx Power 208

U

UPCA 129
  Mesa 123
UPCE0 130
UPCE1 131
User Certificates
  Generating 247
  Installing on MX9 253
User Idle power state 21
User Idle timer 178
User Interface Language 152
Using the Scan Feature 206
Utilities 29

V

Vehicle Cradle 258
Versions 52
Vibrate Indicator 17
Vibration 97

virtual keyboard 148
Volume & Sounds 189

W

Wake Up Event Default Settings 24
Wake up Events 23
Warmboot 182
WAV files 189
WAVPLAY.EXE 30
WEP 198, 229
Windows Certificate Store vs. Certs Path 225
Windows Explorer 37
Wireless Radio
  Summit 274
Wireless Zero Config Utility and the Summit Radio 201
Wordpad 36
WPA-PSK
  Summit Radio 241
WPA/LEAP
  Summit Radio 235, 237
WPA2 198
WWAN 191
WWAN Radio 275